Dépannage de DHCP dans VLAN couche 2 uniquement - Sans fil

Table des matières

- Introduction
- Conditions préalables
  - Exigences
- Présentation de L2 uniquement
  - Aperçu
  - Changement de comportement DHCP dans les VLAN L2 uniquement
  - Multidiffusion Sous-Jacente
  - Diffusion Sur Des Interfaces De Tunnel D'Accès
- Topologie
- Configuration VLAN L2 uniquement
  - Déploiement VLAN L2 uniquement à partir de Catalyst Center
  - Configuration VLAN L2 uniquement - Périphériques du fabric
  - Configuration VLAN L2 uniquement - Contrôleur LAN sans fil
  - Configuration du transfert de couche 2 (périphérie du fabric)
  - Activation de la multidiffusion sans fil
- Flux de trafic DHCP
  - Détection et requête DHCP - Côté sans fil
  - Détection et requête DHCP - Périphérie du fabric
    - Apprentissage MAC avec notification WLC
    - Pontage de diffusion DHCP dans l'inondation de couche 2
    - Captures de paquets
  - Détection et requête DHCP - Frontière L2
    - Captures de paquets
  - Offre DHCP et ACK - Diffusion - Limite L2
    - Formation MAC et enregistrement de passerelle
    - Pontage de diffusion DHCP dans l'inondation de couche 2
  - Offre DHCP et ACK - Diffusion - Périphérie
  - Offre DHCP et ACK - Monodiffusion - Limite L2
  - Offre DHCP et ACK - monodiffusion - périphérie
  - Transaction DHCP - Vérification sans fil

Introduction

Ce document décrit comment dépanner DHCP pour les points d'extrémité sans fil dans un réseau de couche 2 uniquement dans un fabric SD-Access (SDA).

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Transmission IP (Internet Protocol)
- Protocole LISP (Locator/ID Separation Protocol)
- Mode intermédiaire PIM (Protocol Independent Multicast)
- Sans fil compatible Fabric

Configuration matérielle et logicielle requise

- Commutateurs de la gamme Catalyst 9000
- Catalyst Center Version 2.3.7.9
- Contrôleurs LAN sans fil Catalyst 9800
- Points d'accès Catalyst 9100
- Cisco IOS® XE 17.12 et versions ultérieures

Limites

- Une seule limite L2 peut transférer simultanément un VLAN/VNI unique, à moins que des mécanismes robustes de prévention des boucles, tels que FlexLink+ ou des scripts EEM pour désactiver les liaisons, ne soient correctement configurés.

Présentation de L2 uniquement

Aperçu

Dans les déploiements SD-Access classiques, la frontière L2/L3 réside au niveau de la périphérie du fabric (FE), où le FE héberge la passerelle du client sous la forme d'une interface SVI, souvent appelée « passerelle Anycast ». Les VNI de couche 3 (routées) sont établies pour le trafic entre sous-réseaux, tandis que les VNI de couche 2 (commutées) gèrent le trafic intra-sous-réseau. Une configuration homogène sur tous les FE permet une itinérance transparente des clients. Le transfert est optimisé : le trafic intra-sous-réseau (L2) est directement ponté entre les FE, et le trafic inter-sous-réseau (L3) est routé soit entre les FE, soit entre un FE et un noeud périphérique.

Pour les terminaux des fabrics SDA qui nécessitent un point d'entrée réseau strict en dehors du fabric, le fabric SDA doit fournir un canal L2 depuis la périphérie vers une passerelle externe.

Ce concept est analogue aux déploiements de campus Ethernet traditionnels dans lesquels un réseau d’accès de couche 2 se connecte à un routeur de couche 3. Le trafic intra-VLAN reste au sein du réseau L2, tandis que le trafic inter-VLAN est routé par le périphérique L3, qui revient souvent à un VLAN différent sur le réseau L2.

Dans un contexte LISP, le plan de contrôle de site effectue principalement le suivi des adresses MAC et de leurs liaisons MAC-IP correspondantes, à l'instar des entrées ARP traditionnelles. Les

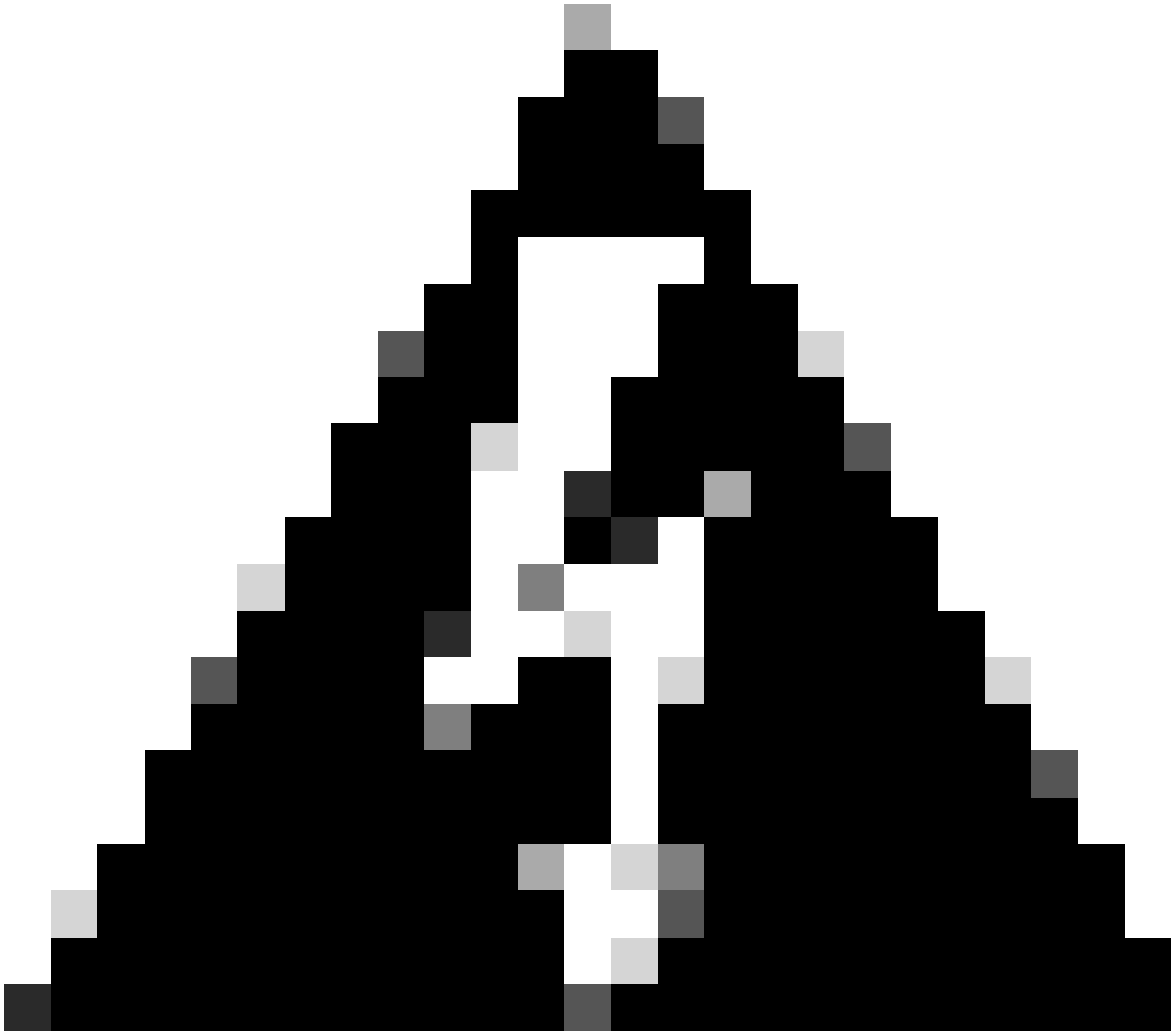
pools L2 VNI/L2 uniquement sont conçus pour faciliter l'enregistrement, la résolution et le transfert exclusivement en fonction de ces deux types d'EID. Par conséquent, tout transfert basé sur le protocole LISP dans un environnement de couche 2 uniquement repose uniquement sur les informations MAC et MAC vers IP, il ignore complètement les EID IPv4 ou IPv6. Pour compléter les EID LISP, les pools de couche 2 uniquement dépendent fortement des mécanismes d'inondation et d'apprentissage, similaires au comportement des commutateurs traditionnels. Par conséquent, l'inondation de couche 2 devient un composant critique pour le traitement du trafic de diffusion, de monodiffusion inconnue et de multidiffusion (BUM) dans cette solution, qui nécessite l'utilisation de la multidiffusion sous-jacente. Inversement, le trafic monodiffusion normal est transféré à l'aide de processus de transfert LISP standard, principalement via Map-Caches.

Les périphéries de fabric et la « périphérie L2 » (L2B) gèrent des VNI L2, qui sont mappés aux VLAN locaux (ce mappage est localement significatif pour les périphériques au sein de SDA, ce qui permet à différents VLAN de mapper au même VNI L2 à travers les noeuds). Dans ce cas d'utilisation spécifique, aucune interface SVI n'est configurée sur ces VLAN au niveau de ces noeuds, ce qui signifie qu'il n'y a pas de VNI L3 correspondant.

Changement de comportement DHCP dans les VLAN L2 uniquement

Dans les pools de passerelles Anycast, le protocole DHCP présente un défi, car chaque périphérie du fabric agit comme passerelle pour ses points d'extrémité connectés directement, avec la même adresse IP de passerelle sur tous les FE. Pour identifier correctement la source d’origine d’un paquet DHCP relayé, les FE doivent insérer l’option DHCP 82 et ses sous-options, y compris les informations RLOC LISP. Cela est possible grâce à la surveillance DHCP sur le VLAN client à la périphérie du fabric. La surveillance DHCP a un double objectif dans ce contexte : il facilite l’insertion de l’option 82 et, surtout, empêche le flot de paquets de diffusion DHCP à travers le domaine de pont (VLAN/VNI). Même lorsque l'inondation de couche 2 est activée pour une passerelle Anycast, la surveillance DHCP supprime efficacement le paquet de diffusion à transférer hors de la périphérie du fabric en tant que diffusion.

En revanche, un VLAN de couche 2 uniquement ne possède pas de passerelle, ce qui simplifie l'identification de la source DHCP. Comme les paquets ne sont relayés par aucune périphérie du fabric, les mécanismes complexes d'identification de la source sont inutiles. Sans la surveillance DHCP sur le VLAN L2 uniquement, le mécanisme de contrôle des inondations pour les paquets DHCP est effectivement contourné. Cela permet aux diffusions DHCP d'être transférées via l'inondation de couche 2 vers leur destination finale, qui peut être un serveur DHCP directement connecté à un noeud de fabric ou un périphérique de couche 3 qui fournit la fonctionnalité de relais DHCP.



Avertissement : La fonctionnalité « Multiple IP to MAC » d'un pool L2 Only active automatiquement la surveillance DHCP en mode Bridge VM, qui applique le contrôle de propagation DHCP. Par conséquent, cela rend le pool VNI de couche 2 incapable de prendre en charge DHCP pour ses points d'extrémité.

Multidiffusion Sous-Jacente

Étant donné que DHCP dépend fortement du trafic de diffusion, la diffusion de couche 2 doit être exploitée pour prendre en charge ce protocole. Comme avec tout autre pool activé pour l'inondation de couche 2, le réseau sous-jacent doit être configuré pour le trafic de multidiffusion, en particulier Any-Source-Multicast utilisant PIM Sparse-Mode. Alors que la configuration multicast sous-jacente est automatisée via le workflow d'automatisation LAN, si cette étape a été omise, une configuration supplémentaire est requise (manuelle ou modèle).

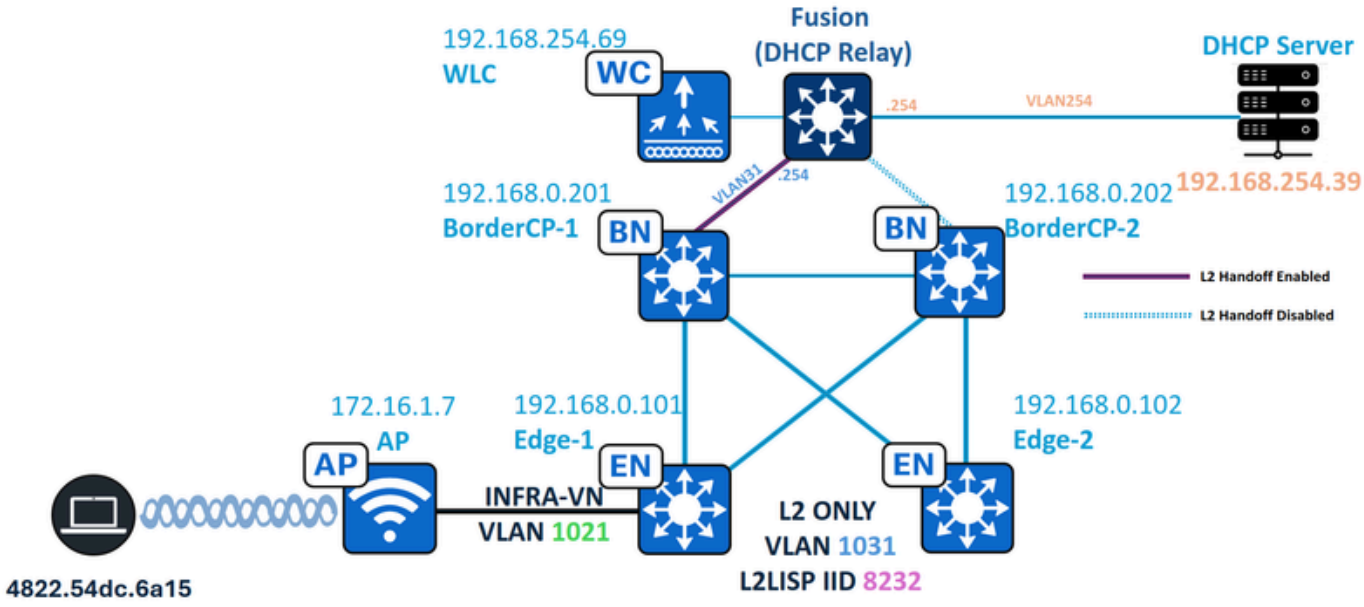
- Activez le routage multidiffusion IP sur tous les noeuds (bordures, bords, noeuds intermédiaires, etc.).
- Configurez PIM Sparse-Mode sur l'interface Loopback0 de chaque noeud Border et Edge.

- Activez le mode intermédiaire PIM sur chaque interface IGP (protocole de routage sous-jacent).
- Configurez le point de rendez-vous PIM (RP) sur tous les noeuds (bordures, bords, noeuds intermédiaires), le placement RP sur les bordures est encouragé.
- Vérifiez les voisins PIM, le RP PIM et l'état du tunnel PIM.

Diffusion Sur Des Interfaces De Tunnel D'Accès

La technologie sans fil compatible avec le fabric utilise la commutation locale et la fonctionnalité VTEP au niveau du point d'accès et du FE. Cependant, une limitation IOS-XE 16.10+ empêche le transfert de diffusion de sortie sur VXLAN vers les points d'accès. Dans les réseaux L2 Only, cela empêche les offres/accusés de réception DHCP d'atteindre les clients sans fil. La fonctionnalité « flood access-tunnel » résout ce problème en activant le transfert de diffusion sur les interfaces de tunnel d'accès de périphérie de fabric.

Topologie



Topologie du réseau

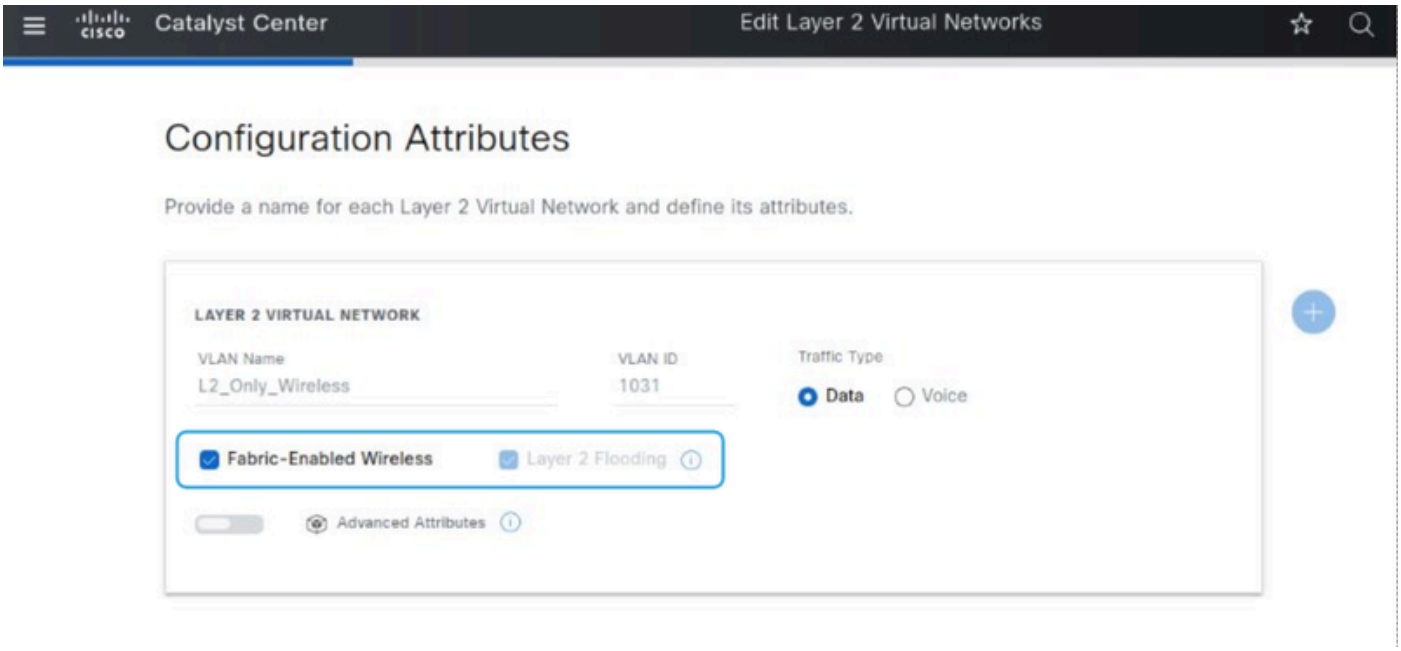
Dans cette topologie :

- 192.168.0.201 et 192.168.0.202 sont des bordures colocalisées pour le site de fabric, BorderCP-1 est la seule bordure avec la fonctionnalité de transfert de couche 2 activée.
- 192.168.0.101 et 192.168.0.102 sont des noeuds de périphérie de fabric
- 172.16.1.7 est le point d'accès dans INFRA-VN avec VLAN 1021
- 192.168.254.39 est le serveur DHCP
- 192.168.254.69 est le contrôleur LAN sans fil
- 4822.54dc.6a15 est le point d'extrémité DHCP
- Le périphérique Fusion joue le rôle de relais DHCP pour les sous-réseaux du fabric.

Configuration VLAN L2 uniquement

Déploiement VLAN L2 uniquement à partir de Catalyst Center

Chemin : Catalyst Center / Provisionnement / Site de fabric / Réseaux virtuels de couche 2 / Modifier les réseaux virtuels de couche 2



Configuration L2VNI avec technologie sans fil compatible avec le fabric

Configuration VLAN L2 uniquement - Périphériques du fabric

Le VLAN des noeuds de périphérie de fabric est configuré avec CTS activé, IGMP et IPv6 MLD désactivés et la configuration LISP L2 requise. Ce pool L2 uniquement est un pool sans fil ; Par conséquent, les fonctionnalités généralement présentes dans les pools sans fil L2 uniquement, telles que RA-Guard, DHCPGuard et Flood Access Tunnel, sont configurées. L'inondation ARP n'est pas activée sur un pool sans fil.

Configuration de la périphérie du fabric (192.168.0.101)

<#root>

```
ipv6 nd raguard policy
```

dnac-sda-permit-nd-raguardv6

```
 device-role router
ipv6 dhcp guard policy
```

dnac-sda-permit-dhcpv6

```
 device-role server

vlan configuration
```

```
1031

 ipv6 nd raguard attach-policy
dnac-sda-permit-nd-raguardv6

 ipv6 dhcp guard attach-policy
dnac-sda-permit-dhcpv6


cts role-based enforcement vlan-list
1031

vlan
1031


name L2_Only_Wireless



ip igmp snooping querier
no ip igmp snooping vlan 1031 querier


no ip igmp snooping vlan 1031


no ipv6 mld snooping vlan 1031



router lisp

 instance-id
8240

  remote-rloc-probe on-route-change
  service ethernet

 eid-table vlan 1031



 broadcast-underlay 239.0.17.1


   flood unknown-unicast
   flood access-tunnel 232.255.255.1 vlan 1021
```

```
   database-mapping mac locator-set rloc_91947dad-3621-42bd-ab6b-379ecebb5a2b
   exit-service-ethernet
```

La commande flood-access tunnel est configurée dans sa variante de réplication de multidiffusion, où tout le trafic de BUM est encapsulé vers les AP en utilisant le groupe de multidiffusion spécifique à la source (232.255.255.1) en utilisant le VLAN de point d'accès INFRA-VN comme VLAN qui est consulté par la surveillance IGMP pour transférer le trafic de BUM.

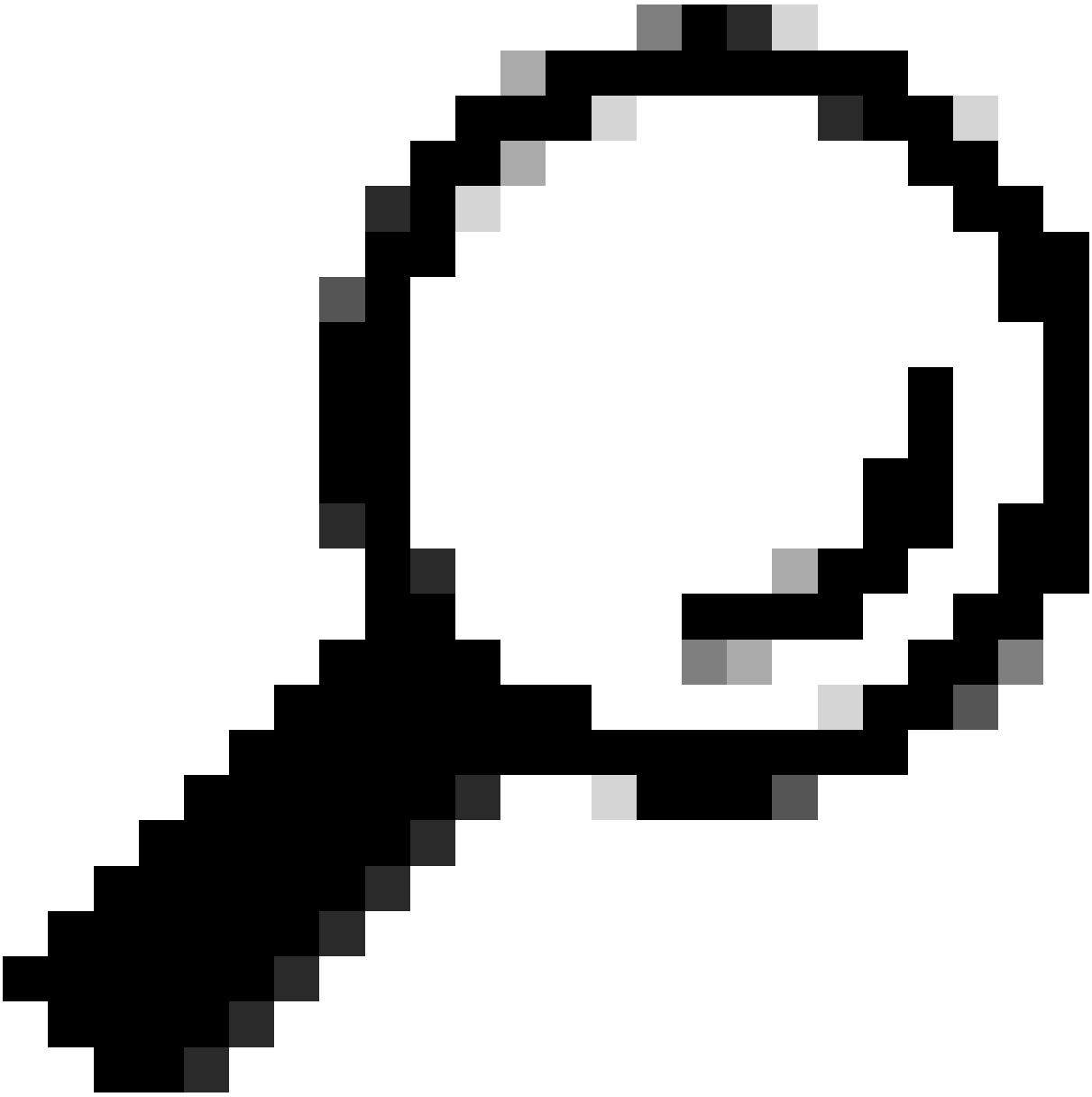
Configuration VLAN L2 uniquement - Contrôleur LAN sans fil

Du côté WLC (Wireless LAN Controller), les balises de site associées aux points d'accès de fabric doivent être configurées avec « no fabric ap-arp-caching » pour désactiver la fonctionnalité proxy-ARP. En outre, « fabric ap-dhcp-broadcast » doit être activé, cette configuration permet aux paquets de diffusion DHCP d'être transférés du point d'accès aux points d'extrémité sans fil.

Configuration WLC de matrice (192.168.254.69)

<#root>

```
wireless tag site RTP-Site-Tag-3
 description "Site Tag RTP-Site-Tag-3"

 no fabric ap-arp-caching
 fabric ap-dhcp-broadcast
```



Conseil : Le groupe de multidiffusion sans fil 232.255.255.1 est le groupe par défaut utilisé par toutes les balises de site.

<#root>

```
WLC#
```

show wireless tag site detailed RTP-Site-Tag-3

```
Site Tag Name        :
```

RTP-Site-Tag-3

```
Description          : Site Tag RTP-Site-Tag-3
---------------------------------------
AP Profile           : default-ap-profile
```

```
Local-site           : Yes
Image Download Profile: default
Fabric AP DHCP Broadcast :
```

Enabled

```
Fabric Multicast Group IPv4 Address :
```

232.255.255.1

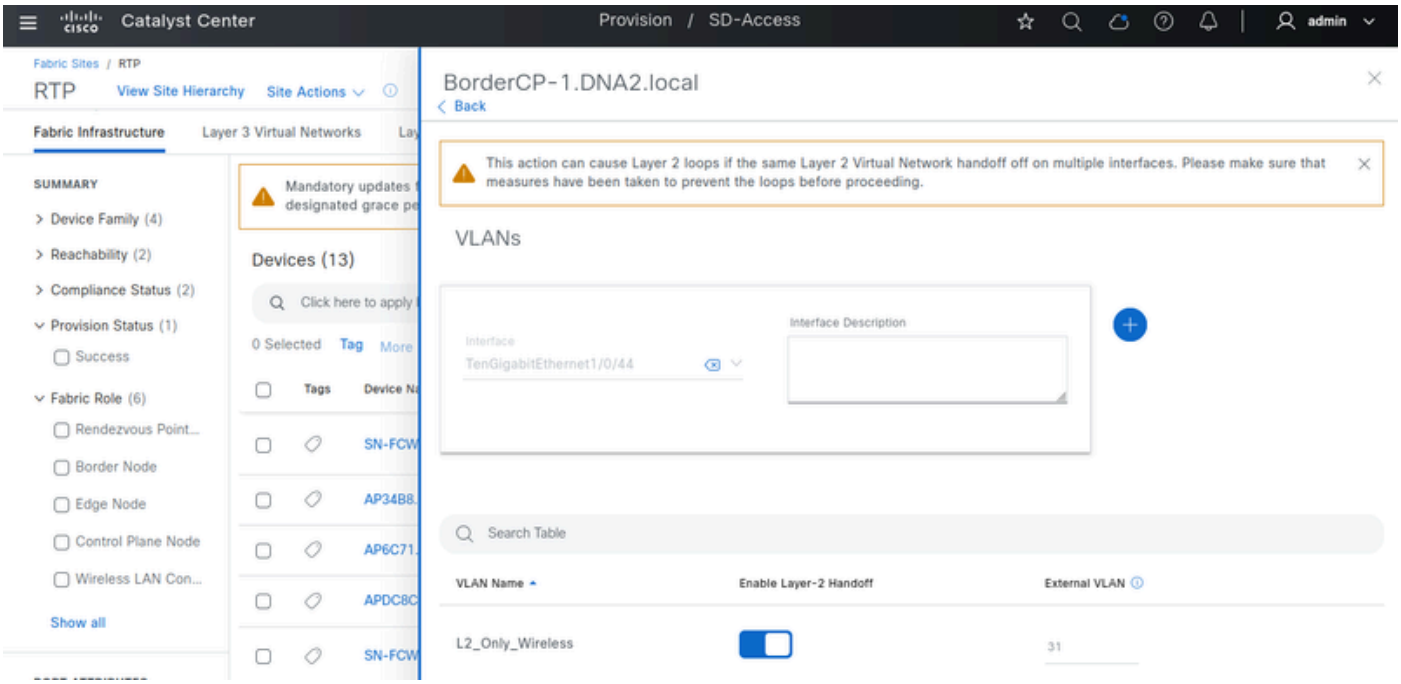
```
RTP-Site-Tag-3 Load : 0
```

Configuration du transfert de couche 2 (périphérie du fabric)

D'un point de vue opérationnel, le serveur DHCP (ou le routeur/relais) est autorisé à être connecté à n'importe quel noeud de fabric, y compris les limites et les bords.

L'utilisation de noeuds en limite pour connecter le serveur DHCP est l'approche recommandée, mais elle nécessite une attention particulière lors de la conception. En effet, la périphérie doit être configurée pour le transfert L2 par interface. Cela permet au pool de fabrics d'être transféré vers le même VLAN qu'au sein du fabric ou vers un autre. Cette flexibilité dans les ID de VLAN entre les périphéries et les bordures de fabric est possible car les deux sont mappés au même ID d'instance LISP de couche 2. Les ports physiques de transfert L2 ne doivent pas être activés simultanément avec le même VLAN pour empêcher les boucles de couche 2 au sein du réseau SD-Access. Pour la redondance, des méthodes telles que StackWise Virtual, FlexLink+ ou des scripts EEM sont nécessaires.

En revanche, la connexion du serveur DHCP ou du routeur de passerelle à une périphérie de fabric ne nécessite aucune configuration supplémentaire.



Configuration de transfert de couche 2

Configuration de la périphérie de fabric/CP (192.168.0.201)

<#root>

```
ipv6 nd raguard policy
dnac-sda-permit-nd-raguardv6

 device-role router
ipv6 dhcp guard policy
dnac-sda-permit-dhcpv6

 device-role server
vlan configuration
3
1

 ipv6 nd raguard attach-policy
dnac-sda-permit-nd-raguardv6

 ipv6 dhcp guard attach-policy
dnac-sda-permit-dhcpv6


cts role-based enforcement vlan-list
31

vlan
3


1


name L2_Only_Wireless



ip igmp snooping querier
no ip igmp snooping vlan 1031 querier


no ip igmp snooping vlan 1031


no ipv6 mld snooping vlan 1031
```

```
router lisp

 instance-id
8240

  remote-rloc-probe on-route-change
  service ethernet

 eid-table vlan 31



 broadcast-underlay 239.0.17.1


   flood unknown-unicast
   flood access-tunnel 232.255.255.1 vlan 1021


   database-mapping mac locator-set rloc_91947dad-3621-42bd-ab6b-379ecebb5a2b
   exit-service-ethernet

interface TenGigabitEthernet1/0/44



switchport mode trunk
<--


DHCP Relay/Server interface
```

Activation de la multidiffusion sans fil

Les bords de fabric sont configurés pour transférer des paquets de diffusion vers des points d'accès via le mécanisme de tunnel d'accès d'inondation. ces paquets sont encapsulés dans le groupe de multidiffusion 232.255.255.1 sur le VLAN INFRA-VN. Les points d'accès rejoignent automatiquement ce groupe de multidiffusion, car leur balise de site est préconfigurée pour l'utiliser.

```
<#root>
WLC#
show ap name AP1 config general | i Site

Site Tag Name                                 :
```

RTP-Site-Tag-3

WLC#

show wireless tag site detailed RTP-Site-Tag-3

Site Tag Name :

RTP-Site-Tag-3

Description : Site Tag RTP-Site-Tag-3

AP Profile : default-ap-profile
Local-site :

Yes

Image Download Profile: default
Fabric AP DHCP Broadcast :

Enabled

Fabric Multicast Group IPv4 Address :

232.255.255.1

RTP-Site-Tag-3 Load : 0

À partir du point d'accès, lors de l'association d'un point d'extrémité sans fil de fabric, un tunnel VXLAN est formé (dynamique du côté du point d'accès, toujours actif du côté de la périphérie du fabric). Dans ce tunnel, le groupe multicast de fabric CAPWAP est vérifié avec des commandes du terminal AP.

<#root>

AP1#

show ip tunnel fabric

Fabric GWs Information:
Tunnel-Id GW-IP GW-MAC Adj-Status Encap-Type Packet-I
n Bytes-In Packet-Out Bytes-out
1

192.168.0.101

00:00:0C:9F:F2:BC

Forward

VXLAN

```
111706302
6 1019814432 1116587492 980205146
AP APP Fabric Information:
GW_ADDR ENCAP_TYPE VNID SGT FEATURE_FLAG GW_SRC_MAC GW_DST_MAC

AP1#
```

show capwap mcast

```
IPv4 Multicast:
Vlan      Group IP Version      Query Timer   Sent QRV left Port
   0
```

232.255.255.1

```
       2 972789.691334200 140626        2    0
```

Du côté de la périphérie du fabric, vérifiez que la surveillance IGMP est activée pour le VLAN AP INFRA-VN, que les points d'accès ont formé une interface de tunnel d'accès et qu'ils ont rejoint le groupe de multidiffusion 232.255.255.1

<#root>

```
Edge-1#
```

show ip igmp snooping vlan 1021 | i IGMP

```
Global IGMP Snooping configuration:
IGMP snooping                :
```

Enabled

```
IGMPv3 snooping              :
```

Enabled

```
IGMP snooping                       :
```

Enabled

```
IGMPv2 immediate leave              : Disabled
CGMP interoperability mode          : IGMP_ONLY

Edge-1#
```

show ip igmp snooping groups vlan

1021 232.255.255.1

```
Vlan      Group                     Type        Version     Port List
------------------------------------------------------------------------
```

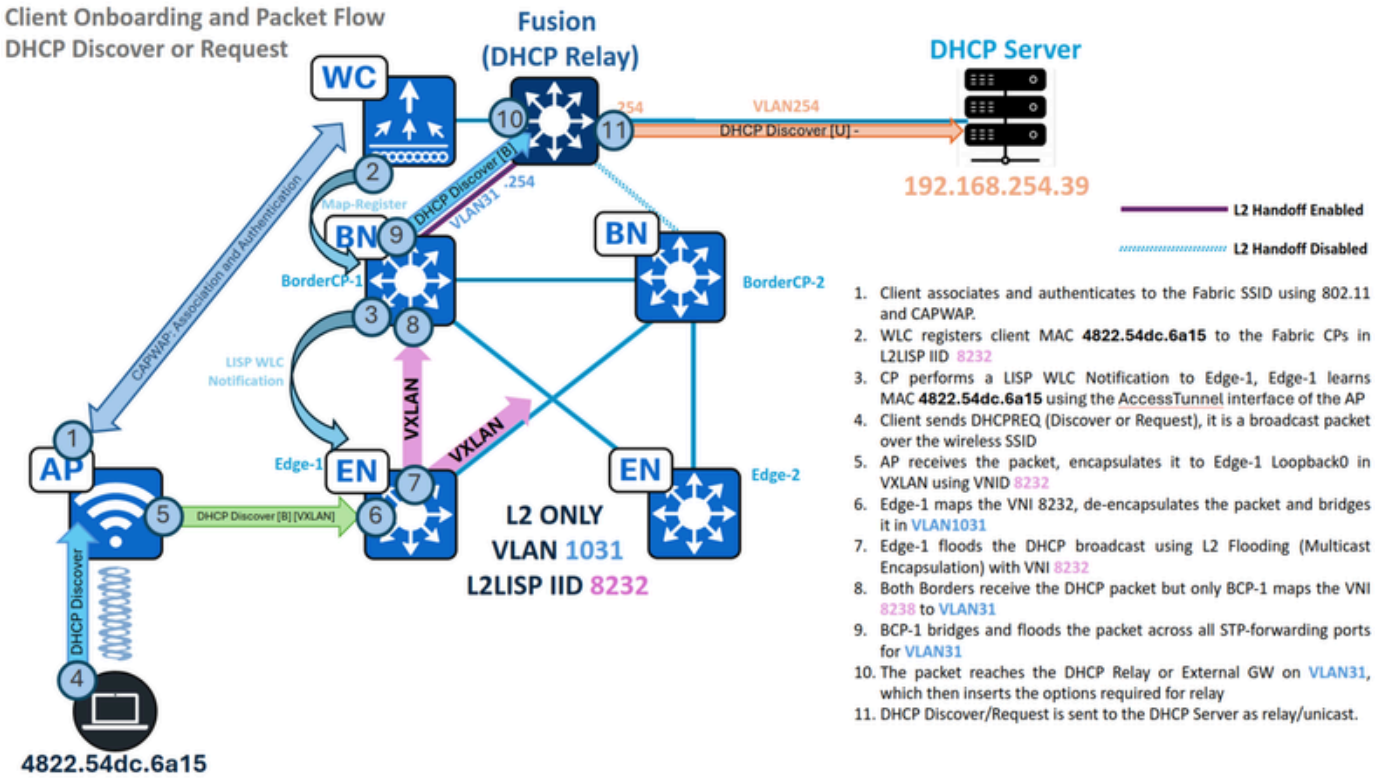
1021   232.255.255.1

```
           igmp        v2
 Te1/0/12   ----- Access Point Port


Edge-1#
show device-tracking database interface te1/0/12 | be Network


   Network Layer Address                    Link Layer Address
Interface  vlan       prlvl      age        state      Time left


DH4 172.16.1.7

                             dc8c.3756.99bc

Te1/0/12   1021

      0024       1s         REACHABLE  251 s(76444 s)
Edge-1#
show access-tunnel summary


Access Tunnels General Statistics:
  Number of AccessTunnel Data Tunnels       = 1
Name    RLOC IP(Source)  AP IP(Destination)  VRF ID  Source Port  Destination Port
------  ---------------  ------------------  ------  -----------  ----------------


Ac2



192.168.0.101



172.16.1.7

       0       N/A          4789
<snip>
```

Ces vérifications confirment la réussite de l'activation de la multidiffusion sans fil sur le point d'accès, la périphérie du fabric et le contrôleur LAN sans fil.

Flux de trafic DHCP

Détection et requête DHCP - Côté sans fil



Flux de trafic - Détection et requête DHCP dans L2 uniquement

identifier l'état du point d'extrémité sans fil, son point d'accès connecté et les propriétés de fabric associées.

<#root>

```
WLC#
show wireless client summary | i MAC|-|4822.54dc.6a15

MAC Address    AP Name                                          Type ID   State            Protocol Meth
-------------------------------------------------------------------------------------------------------

4822.54dc.6a15

AP1

                              WLAN

17

Run

               11n(2.4) MAB        Local

WLC#
show wireless client mac 4822.54dc.6a15 detail | se AP Name|Policy Profile|Fabric

AP Name:
```

AP1

Policy Profile :

RTP_POD1_SSID_profile

Fabric status :

Enabled

  RLOC   :

192.168.0.101

  VNID   :

8232

  SGT   : 0
  Control plane name :

default-control-plane

Il est important de vérifier que les fonctionnalités de commutation centrale et dhcp centrale sont toutes deux désactivées sur le profil de stratégie. Les commandes « no central dhcp » et « no central switching » doivent être configurées sur le profil de stratégie pour le SSID.

<#root>

WLC#

show wireless profile policy detailed RTP_POD1_SSID_profile | i Central

  Flex Central Switching   : DISABLED

  Flex Central Authentication   : ENABLED

 Flex Central DHCP   : DISABLED

  VLAN based Central Switching   : DISABLED

Ces vérifications confirment que le point d'extrémité est connecté à « AP1 », qui est associé au RLOC de périphérie de fabric 192.168.0.101. Par conséquent, son trafic est encapsulé via VXLAN avec le VNID 8232 pour être transmis du point d'accès à la périphérie de fabric.

Détection et requête DHCP - Périphérie du fabric

Apprentissage MAC avec notification WLC

Lors de l'intégration du point d'extrémité, le WLC enregistre l'adresse MAC du point d'extrémité sans fil dans le plan de contrôle du fabric. Simultanément, le plan de contrôle indique au noeud Périphérie du fabric (auquel le point d'accès est connecté) de créer une entrée d'apprentissage MAC « CP_LEARN » spéciale, pointant vers l'interface de tunnel d'accès du point d'accès.

<#root>

Edge-1#

show lisp session

Sessions for VRF default, total: 2, established: 2
Peer State Up/Down In/Out Users

192.168.0.201:4342 Up

2w2d 806/553 44

192.168.0.202:4342 Up

2w2d 654/442 44

Edge-1#

show lisp instance-id 8232 ethernet database wlc 4822.54dc.6a15

WLC clients/access-points information for LISP 0 EID-table Vlan

1031

(IID

8232

)
Hardware Address:

4822.54dc.6a15

Type: client
Sources: 2
Tunnel Update: Signalled
Source MS:

192.168.0.201

RLOC:

192.168.0.101

Up time: 1w6d
Metadata length: 34
Metadata (hex): 00 01 00 22 00 01 00 0C AC 10 01 07 00 00 10 01
00 02 00 06 00 00 00 03 00 0C 00 00 00 00 68 99

```
                  6A D2

Edge-1#
```

show mac address-table address 4822.54dc.6a15

```
          Mac Address Table
-------------------------------------------
Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
```

1031

4822.54dc.6a15

CP_LEARN

Ac2

Si l'adresse MAC du point d'extrémité est correctement apprise via l'interface de tunnel d'accès correspondant à son point d'accès connecté, cette étape est considérée comme terminée.

Pontage de diffusion DHCP dans l'inondation de couche 2

Lorsque la surveillance DHCP est désactivée, les diffusions DHCP ne sont pas bloquées ; au lieu de cela, ils sont encapsulés en multidiffusion pour l'inondation de couche 2. Inversement, l'activation de la surveillance DHCP empêche l'inondation de ces paquets de diffusion.

<#root>

```
Edge-1#
```

show ip dhcp snooping

Switch DHCP snooping isenabled

```
Switch DHCP gleaning is disabled
DHCP snooping is configured on following VLANs:
12-13,50,52-53,333,1021-1026
```

DHCP snooping isoperationalon following VLANs:

12-13,50,52-53,333,1021-1026

<--

VLAN1031 should not be listed, as DHCP snooping must be disabled in L2 Only pools.

```
 Proxy bridge is configured on following VLANs:
1024
 Proxy bridge is operational on following VLANs:
1024
<snip>
```

La surveillance DHCP étant désactivée, la détection/requête DHCP utilise l'interface L2LISP0, pontant le trafic via l'inondation L2. Selon la version de Catalyst Center et les bannières de fabric appliquées, les listes d'accès de l'interface L2LISP0 peuvent être configurées dans les deux directions ; Par conséquent, assurez-vous que le trafic DHCP (ports UDP 67 et 68) n'est pas explicitement refusé par les entrées de contrôle d'accès (ACE).

<#root>

interface L2LISP0

 ip access-group

SDA-FABRIC-LISP

in

 ip access-group

SDA-FABRIC-LISP out

Edge-1#

show access-list SDA-FABRIC-LISP

```
Extended IP access list SDA-FABRIC-LISP
    10 deny ip any host 224.0.0.22
    20 deny ip any host 224.0.0.13
    30 deny ip any host 224.0.0.1
```

40 permit ip any any

Utilisez le groupe broadcast-underlay configuré pour l'instance L2LISP et l'adresse IP Loopback0 du périmètre du fabric pour vérifier l'entrée de diffusion de couche 2 (S, G) qui relie ce paquet à d'autres noeuds du fabric. Consultez les tables mroute et mfib pour valider les paramètres tels que l'interface entrante, la liste des interfaces sortantes et les compteurs de transfert.

<#root>

Edge-1#

show ip interface loopback 0 | i Internet

```
  Internet address is
192.168.0.101/32


Edge-1#
show running-config | se 8232

interface L2LISP0.8232
instance-id 8232

  remote-rloc-probe on-route-change
  service ethernet
   eid-table vlan 1031

 broadcast-underlay 239.0.17.1


Edge-1#
show ip mroute 239.0.17.1 192.168.0.101 | be \(


(192.168.0.101, 239.0.17.1)
, 00:00:19/00:03:17, flags: FT
  Incoming interface:
Null0
, RPF nbr 0.0.0.0
<--

Local S,G IIF must be Null0

  Outgoing interface list:

 TenGigabitEthernet1/1/2
,
Forward
/Sparse, 00:00:19/00:03:10, flags:
<--

1st OIF = Te1/1/2 = Border2 Uplink


 TenGigabitEthernet1/1/1
```

,

Forward

/Sparse, 00:00:19/00:03:13, flags:

<--

2nd OIF = Te1/1/1 = Border1 Uplink

Edge-1#

show ip mfib 239.0.17.1 192.168.0.101 count

Forwarding Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kilobits per second
Other counts: Total/RPF failed/Other drops(OIF-null, rate-limit etc)
Default
 13 routes, 6 (*,G)s, 3 (*,G/m)s
Group:

239.0.17.1

  Source:

192.168.0.101

,
   SW Forwarding: 1/0/392/0, Other: 1/1/0
   HW Forwarding:

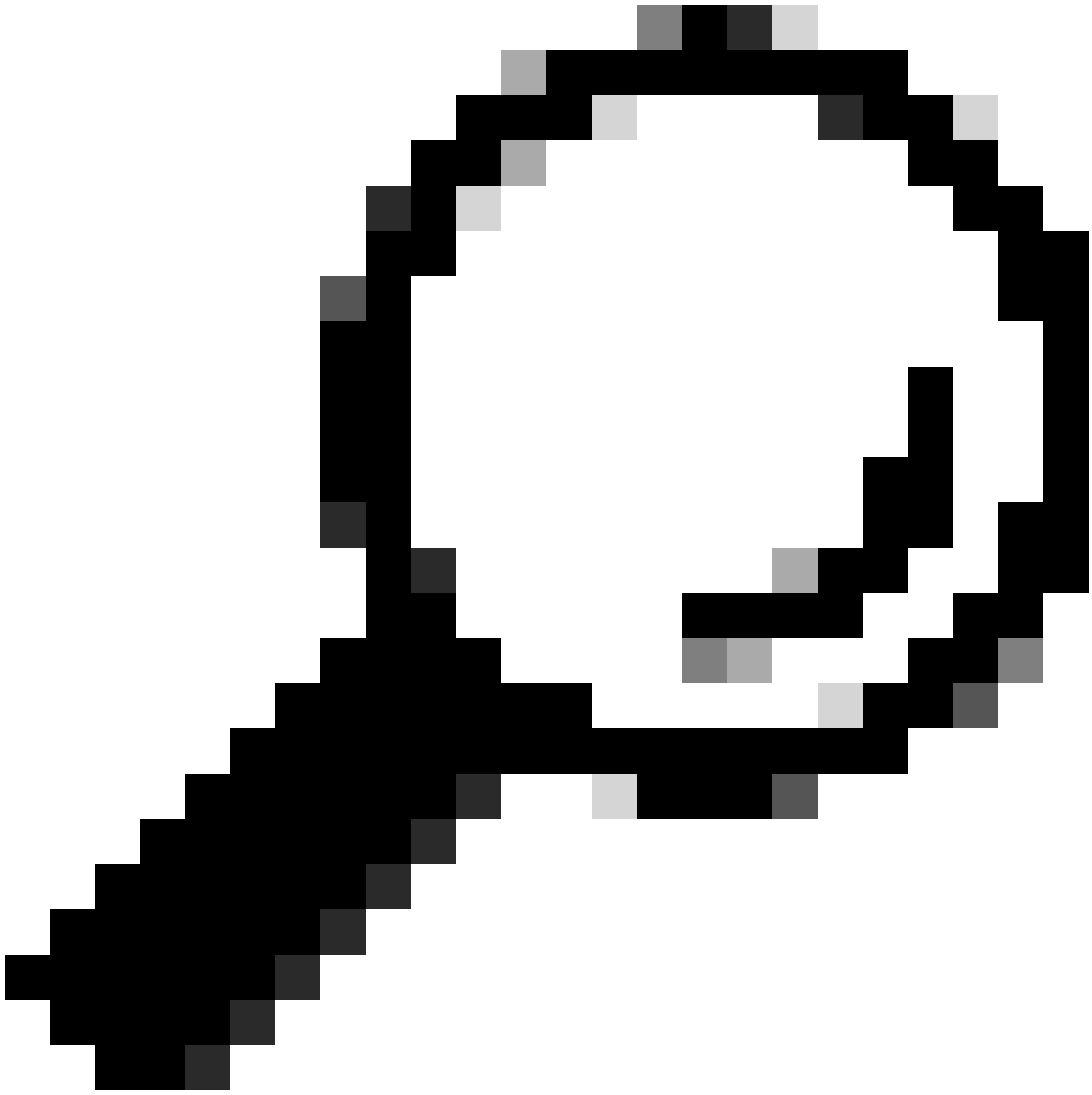
7

/0/231/0, Other: 0/0/0

<--

HW Forwarding counters (First counter = Pkt Count) must increase

  Totals - Source count: 1, Packet count: 8



Conseil : Conseil : Si aucune entrée (S, G) n'est trouvée ou si la liste d'interfaces sortantes (OIL) ne contient aucune interface sortante (OIF), cela indique un problème avec la configuration ou l'opération de multidiffusion sous-jacente.

Captures de paquets

Configurez une capture de paquet intégrée simultanée sur le commutateur pour enregistrer à la fois le paquet DHCP entrant du point d'accès et le paquet de sortie correspondant pour l'inondation de couche 2.

Captures de paquets Fabric Edge (192.168.0.101)

```
monitor capture cap interface TenGigabitEthernet1/0/12 IN    <-- Access Point Port

monitor capture cap interface TenGigabitEthernet1/1/1 OUT    <-- Multicast Route (L2 Flooding) OIF

monitor capture cap match any

monitor capture cap buffer size 100

monitor capture cap limit pps 1000

monitor capture cap start

monitor capture cap stop
```

Lors de la capture de paquets, trois paquets distincts doivent être observés :

- Détection DHCP - VXLAN - AP vers périphérie
- Détection DHCP - CAPWAP - AP vers WLC
- Détection DHCP - VXLAN - Groupe de périphérie à multidiffusion

<#root>

```
Edge-1#

show monitor capture cap buffer display-filter "bootp and dhcp.hw.mac_addr==4822.54dc.6a15"

<-- 4822.54dc.6a15 is the endpoint MAC


Starting the packet display ........ Press Ctrl + Shift + 6 to exit
  129   4.865410      0.0.0.0 -> 255.255.255.255 DHCP

394

 DHCP Discover - Transaction ID 0x824bdf45

<--

 From AP to Edge


  130   4.865439      0.0.0.0 -> 255.255.255.255 DHCP

420

 DHCP Discover - Transaction ID 0x824bdf45

<--

 From AP to WLC
```

```
  131   4.865459      0.0.0.0 -> 255.255.255.255 DHCP
```

394

```
 DHCP Discover - Transaction ID 0x824bdf45
```

<--

From Edge to L2 Flooding Group

```
Edge-1#
```

show monitor capture cap buffer display-filter "bootp and dhcp.hw.mac_addr==4822.54dc.6a15

and vxlan"

```
Starting the packet display ........ Press Ctrl + Shift + 6 to exit
  129   4.865410      0.0.0.0 -> 255.255.255.255 DHCP
```

394

```
 DHCP Discover - Transaction ID 0x824bdf45
  131   4.865459      0.0.0.0 -> 255.255.255.255 DHCP
```

394

```
 DHCP Discover - Transaction ID 0x824bdf45
Edge-1#
```

show monitor capture cap buffer display-filter "bootp and dhcp.hw.mac_addr==4822.54dc.6a15

and udp.port==5247"

```
Starting the packet display ........ Press Ctrl + Shift + 6 to exit
  130   4.865439      0.0.0.0 -> 255.255.255.255 DHCP
```

420

```
 DHCP Discover - Transaction ID 0x824bdf45
Edge-1#
```

show monitor capture cap buffer display-filter "bootp and dhcp.hw.mac_addr==4822.54dc.6a15 and vxlan"

detail

| i Internet

```
Internet Protocol Version 4, Src:
```

172.16.1.7

```
, Dst:
```

192.168.0.101   <-- From AP to Edge

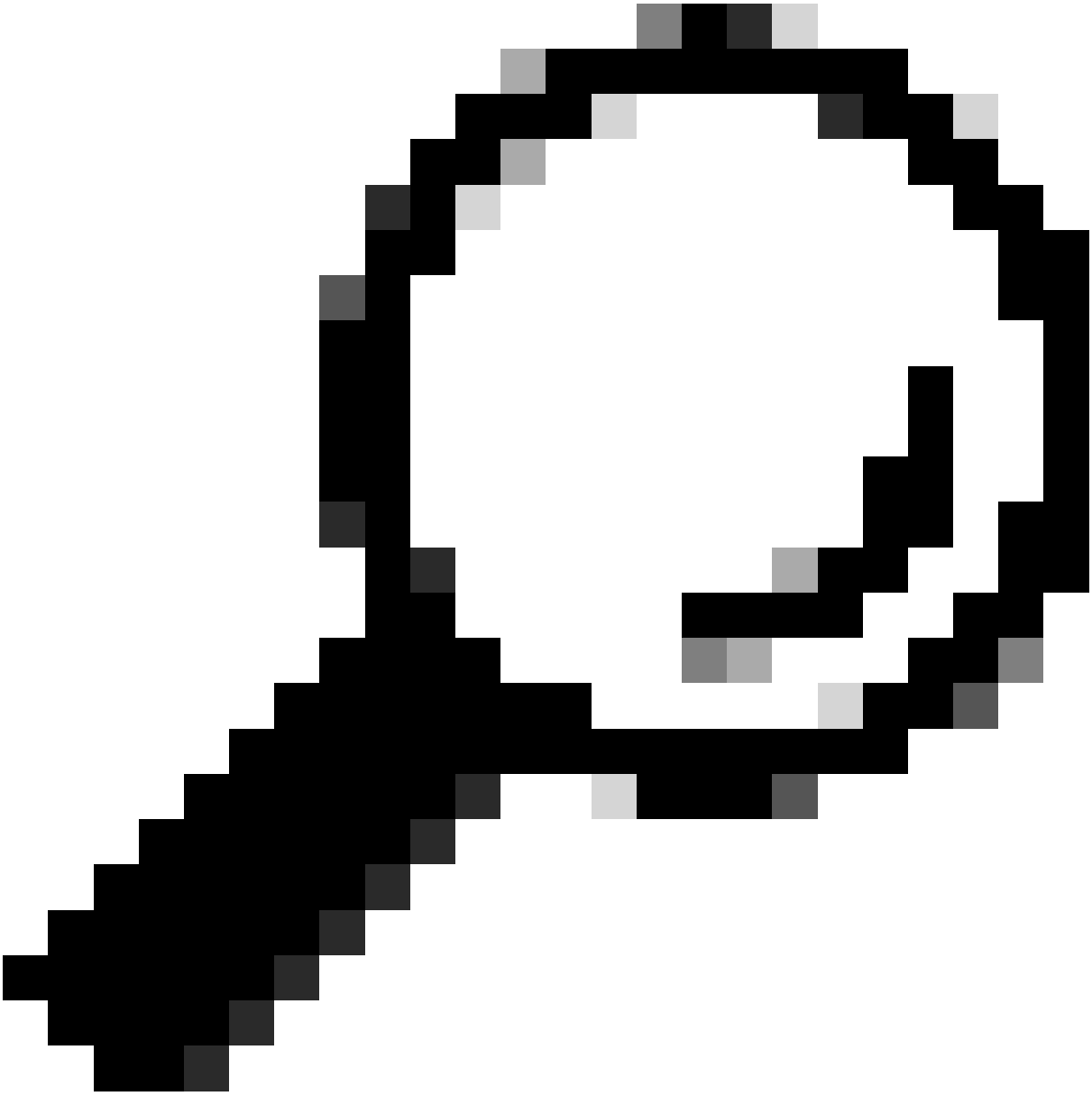
```
Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
Internet Protocol Version 4, Src:
```

192.168.0.101

, Dst:

239.0.17.1 <-- From Edge to Upstream (Layer 2 Flooding)

Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255



Conseil : Sur les réseaux sans fil activés par le fabric, les paquets encapsulés VXLAN transmettent le trafic DHCP aux clients ou aux serveurs. Cependant, les paquets encapsulés CAPWAP DATA (UDP 5247) transmettent au WLC uniquement à des fins de suivi, telles que l'état IP Learn ou le suivi de périphérique sans fil.

Détection et requête DHCP - Frontière L2

Une fois que le périphérique a envoyé les paquets de détection et de requête DHCP via l'inondation de couche 2, encapsulés avec le groupe de diffusion sous-jacente 239.0.17.1, ces paquets sont reçus par la frontière de transfert de couche 2, en particulier Border/CP-1 dans ce scénario.

Pour que cela se produise, Border/CP-1 doit posséder une route de multidiffusion avec le (S, G) de la périphérie, et sa liste d'interfaces sortantes doit inclure l'instance L2LISP du VLAN de transfert de couche 2. Il est important de noter que les bordures de transfert L2 partagent le même ID d'instance L2LISP, même si elles utilisent des VLAN différents pour le transfert.

<#root>

BorderCP-1#

show vlan id 31

VLAN Name Status Ports
---- -------------------------------- --------- --------------------------------

31

L2_Only_Wireless

active

L2LI0:

8232

,

Te1/0/44

BorderCP-1#

show ip mroute 239.0.17.1 192.168.0.101 | be \(

(

192.168.0.101

,

239.0.17.1

), 00:03:20/00:00:48, flags: MTA
Incoming interface:

TenGigabitEthernet1/0/42

, RPF nbr 192.168.98.3

<-- IIF Te1/0/42 is the RPF interface for 192.168.0.101 (Edge RLOC)

```
  Outgoing interface list:
   TenGigabitEthernet1/0/26, Forward/Sparse, 00:03:20/00:03:24, flags:
```

L2LISP0.8232

```
, Forward/Sparse-Dense, 00:03:20/00:02:39, flags:

BorderCP-1#
```

show ip mfib 239.0.17.1 192.168.0.101 count

```
Forwarding Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kilobits per second
Other counts:      Total/RPF failed/Other drops(OIF-null, rate-limit etc)
Default
 13 routes, 6 (*,G)s, 3 (*,G/m)s
Group:
```

239.0.17.1

```
  Source:
```

192.168.0.101,

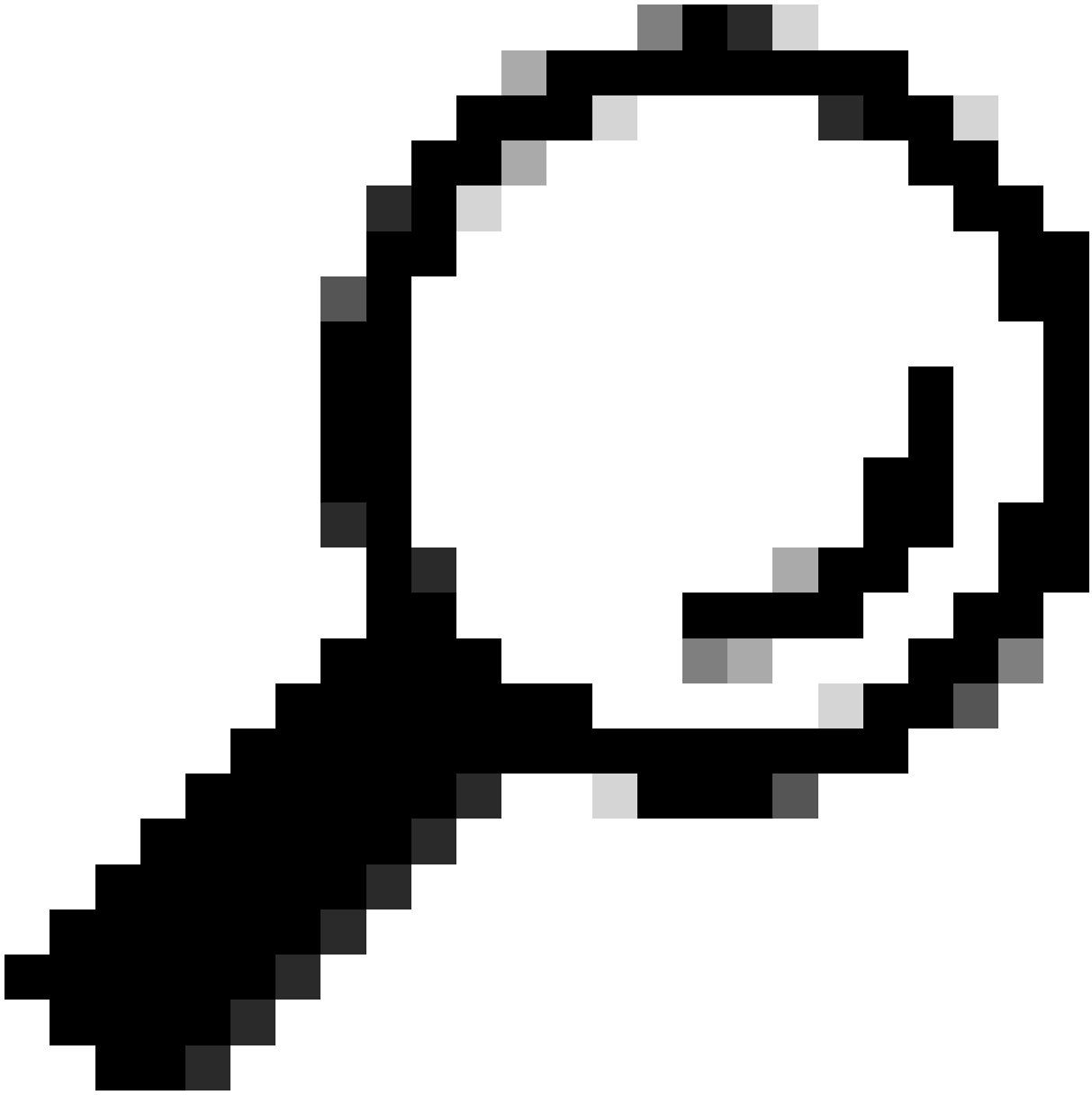
```
   SW Forwarding: 1/0/392/0, Other: 0/0/0
   HW Forwarding:
```

3

```
/0/317/0, Other: 0/0/0
```

<-- HW Forwarding counters (First counter = Pkt Count) must increase

```
  Totals - Source count: 1, Packet count: 4
```



Conseil : Si une entrée (S, G) est introuvable, cela indique un problème avec la configuration ou l'opération de multidiffusion sous-jacente. Si le L2LISP de l'instance requise n'est pas présent en tant qu'OIF, cela indique un problème avec l'état de fonctionnement UP/DOWN de la sous-interface L2LISP ou l'état d'activation IGMP de l'interface L2LISP.

Comme pour le noeud Périphérie du fabric, assurez-vous qu'aucune entrée de contrôle d'accès ne refuse le paquet DHCP entrant sur l'interface L2LISP0.

<#root>

```
BorderCP-1#
```

show ip access-lists SDA-FABRIC-LISP

```
Extended IP access list SDA-FABRIC-LISP
    10 deny ip any host 224.0.0.22
    20 deny ip any host 224.0.0.13
    30 deny ip any host 224.0.0.1

40 permit ip any any
```

Une fois que le paquet est désencapsulé et placé sur le VLAN correspondant à VNI 8240, sa nature de diffusion indique qu'il est diffusé par tous les ports de transfert du protocole Spanning Tree pour le VLAN 141 de transfert.

<#root>

```
BorderCP-1#

show spanning-tree vlan 31 | be Interface

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------

Te1/0/44

          Desg

FWD

 2000      128.56   P2p
```

La table Device-Tracking confirme que l'interface Te1/0/44, qui se connecte au modem routeur/relais DHCP, doit être un port de transfert STP.

<#root>

```
BorderCP-1#

show device-tracking database address 172.16.141.254 | be Network

  Network Layer Address                    Link Layer Address
Interface  vlan       prlvl      age        state      Time left
ARP

172.16.131.254

                        f87b.2003.7fd5

Te1/0/44


 31

       0005       34s       REACHABLE  112 s try 0
```

Captures de paquets

Configurez une capture de paquets intégrée simultanée sur le commutateur pour enregistrer à la fois le paquet DHCP entrant provenant de l'inondation de couche 2 (interface S, G entrante) et le paquet de sortie correspondant vers le relais DHCP. Lors de la capture de paquets, deux paquets distincts doivent être observés : le paquet encapsulé VXLAN de Edge-1 et le paquet désencapsulé qui va au relais DHCP.

Captures de paquets Fabric Border/CP (192.168.0.201)

<#root>

```
monitor capture cap interface TenGigabitEthernet1/0/42 IN

<--

 Ingress interface for Edge's S,G Mroute (192.168.0.101, 239.0.17.1)


monitor capture cap interface TenGigabitEthernet1/0/44 OUT    <-- Interface that connects to the DHCP Re


monitor capture cap match any

monitor capture cap buffer size 100


monitor capture cap start


monitor capture cap stop


BorderCP-1#

show monitor capture cap buffer display-filter "bootp and dhcp.hw.mac_addr==4822.54dc.6a15"


Starting the packet display ........ Press Ctrl + Shift + 6 to exit
  324  16.695022      0.0.0.0 -> 255.255.255.255 DHCP

394

 DHCP Discover - Transaction ID 0x824bdf45

<-- 394 is the Lenght of the VXLAN encapsulated packet

  325  10.834141      0.0.0.0 -> 255.255.255.255 DHCP

420

 DHCP Discover - Transaction ID 0x168bd882

<-- 420 is the Lenght of the CAPWAP encapsulated packet
```

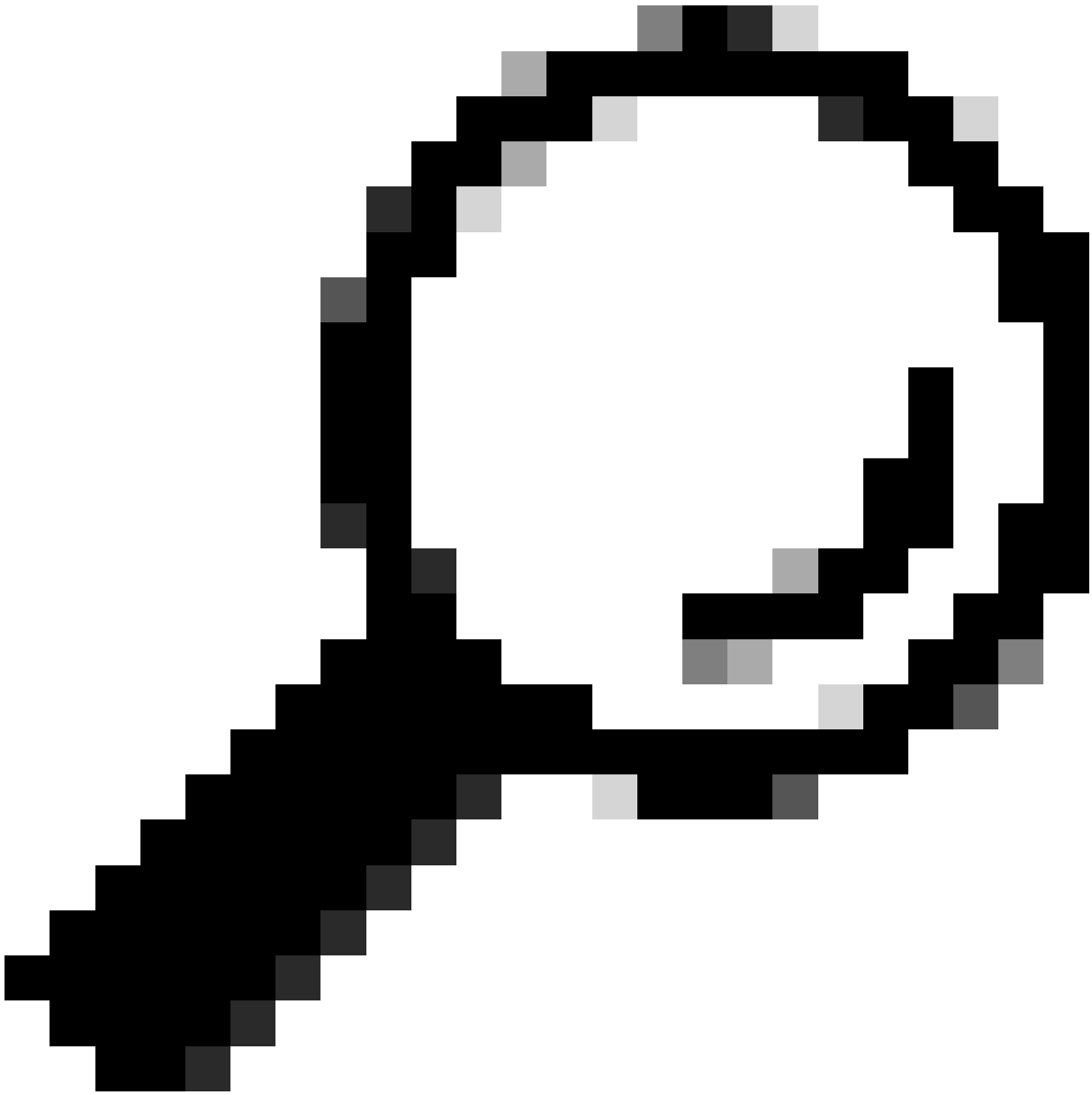
```
  326  16.695053      0.0.0.0 -> 255.255.255.255 DHCP
352
 DHCP Discover - Transaction ID 0x824bdf45
<-- 352 is the Lenght of the VXLAN encapsulated packet



Packet 324: VXLAN Encapsulated

BorderCP-1#
show monitor capture cap buffer display-filter "frame.number==324" detail | i Internet
Internet Protocol Version 4, Src:
192.168.0.101, Dst: 239.0.17.1

Internet Protocol Version 4, Src:
 0.0.0.0, Dst: 255.255.255.255



Packet 326: Plain (dot1Q cannot be captured at egress due to EPC limitations)

BorderCP-1#
show monitor capture cap buffer display-filter "frame.number==326" detailed | i Internet
Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
```

À ce stade, le paquet Discover/Request a quitté le fabric SD-Access, concluant cette section. Cependant, avant de continuer, un paramètre crucial (l'indicateur de diffusion DHCP, déterminé par le point d'extrémité lui-même) dicte le scénario de transfert pour les paquets Offer ou ACK suivants. Nous pouvons examiner l'un de nos paquets de détection pour inspecter cet indicateur.

<#root>

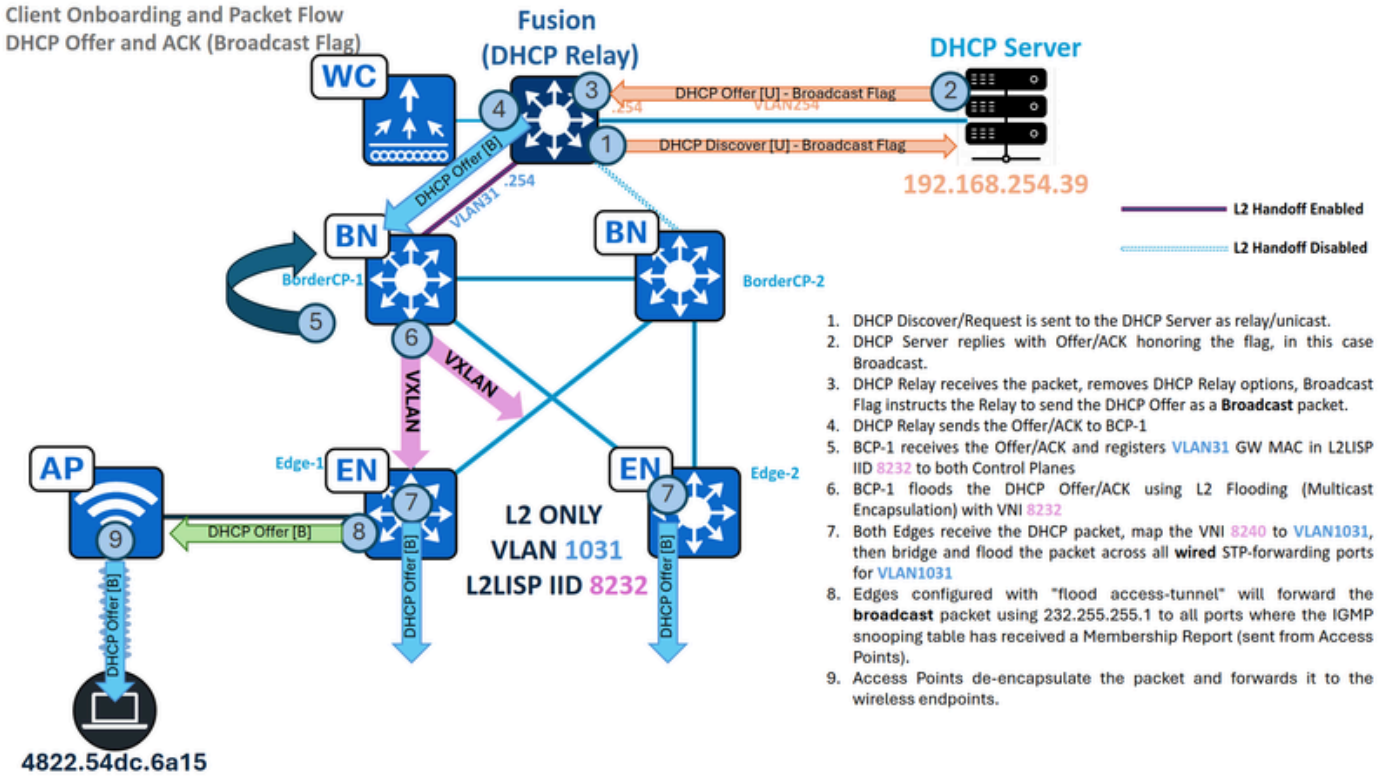
```
BorderCP-1#
show monitor capture cap buffer display-filter "bootp.type==1 and dhcp.hw.mac_addr==4822.54dc.6a15
" detailed | sect Dynamic


Dynamic Host Configuration Protocol (Discover)

    Message type: Boot Request (1)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
```

```
    Transaction ID: 0x00002030
    Seconds elapsed: 3

Bootp flags: 0x8000, Broadcast flag (Broadcast)


1... .... .... .... = Broadcast flag: Broadcast   <-- Broadcast Flag set by the Endpoint

        .000 0000 0000 0000 = Reserved flags: 0x0000
```



Conseil : Le bootp.type==1 peut être utilisé pour filtrer uniquement les paquets de détection et de requête.

Offre DHCP et ACK - Diffusion - Limite L2



Flux de trafic - Offre DHCP de diffusion et ACK dans L2 uniquement

Maintenant que la découverte DHCP a quitté le fabric SD-Access, le relais DHCP insère les options de relais DHCP traditionnelles (par exemple, GiAddr/GatewayIPAddress) et transfère le paquet en tant que transmission monodiffusion au serveur DHCP. Dans ce flux, le fabric SD-Access n'ajoute aucune option DHCP spéciale.

Lors de l'arrivée d'une détection/requête DHCP au serveur, ce dernier honore l'indicateur de diffusion ou de monodiffusion intégré. Cet indicateur indique si l'agent de relais DHCP transfère l'offre DHCP au périphérique en aval (nos frontières) en tant que trame de diffusion ou de monodiffusion. Pour cette démonstration, un scénario de diffusion est supposé.

Formation MAC et enregistrement de passerelle

Lorsque le relais DHCP envoie une offre ou un accusé de réception DHCP, le noeud L2BN doit apprendre l'adresse MAC de la passerelle, l'ajouter à sa table d'adresses MAC, puis à la table SISF L2/MAC, et enfin à la base de données L2LISP pour VLAN 141, mappée à l'instance L2LISP 8232.

<#root>

```
BorderCP-1#
```

```
show mac address-table interface te1/0/44
```

```
          Mac Address Table
-------------------------------------------
```

```
Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

31


f87b.2003.7fd5

    DYNAMIC

Te1/0/44

BorderCP-1#

show vlan id 31

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------


31

  L2_Only_Wireless               active    L2LI0:

8232

,

Te1/0/44

BorderCP-1#

show device-tracking database mac | i 7fd5|vlan

 MAC                    Interface  vlan       prlvl      state            Time left        Policy

 f87b.2003.7fd5


 Te1/0/44    31

        NO TRUST

 MAC-REACHABLE

    61 s             LISP-DT-GLEAN-VLAN 64

BorderCP-1#

show lisp ins 8232 dynamic-eid summary | i Name|f87b.2003.7fd5

Dyn-EID Name         Dynamic-EID      Interface     Uptime    Last      Pending

Auto-L2-group-8232


f87b.2003.7fd5
```

```
 N/A           6d06h     never

  0


BorderCP-1#

show lisp instance-id 8232 ethernet database

f87b.2003.7fd5


LISP ETR MAC Mapping Database for LISP 0 EID-table Vlan

31

 (IID

8232

), LSBs: 0x1
Entries total 1, no-route 0, inactive 0, do-not-register 0


f87b.2003.7fd5/48

,
 dynamic-eid Auto-L2-group-8240, inherited from default locator-set
rloc_0f43c5d8-f48d-48a5-a5a8-094b87f3a5f7, auto-discover-rlocs
  Uptime: 6d06h, Last-change: 6d06h
  Domain-ID: local
  Service-Insertion: N/A
  Locator        Pri/Wgt  Source     State


 192.168.0.201

  10/10   cfg-intf   site-self, reachable
  Map-server     Uptime         ACK  Domain-ID


192.168.0.201

 6d06h

Yes

  0


192.168.0.202

  6d06h

Yes

  0
```

Si l'adresse MAC de la passerelle est correctement apprise et que l'indicateur ACK a été marqué comme "Oui" pour les plans de contrôle de fabric, cette étape est considérée comme terminée.

Pontage de diffusion DHCP dans l'inondation de couche 2

Sans la surveillance DHCP activée, les diffusions DHCP ne sont pas bloquées et sont encapsulées en multidiffusion pour l'inondation de couche 2. Inversement, si la surveillance DHCP est activée, le flux de paquets de diffusion DHCP est empêché.

<#root>

BorderCP-1#

show ip dhcp snooping

Switch DHCP snooping is enabled

Switch DHCP gleaning is disabled
DHCP snooping is configured on following VLANs:
1001

DHCP snooping is operational on following VLANs:

1001 <-- VLAN31 should not be listed, as DHCP snooping must be disabled in L2 Only pools.

Proxy bridge is configured on following VLANs:
none
Proxy bridge is operational on following VLANs:
none

La surveillance DHCP n'étant pas activée dans l'environnement L2Border, la configuration de l'approbation de surveillance DHCP n'est pas nécessaire.

À ce stade, la validation des listes de contrôle d’accès L2LISP est déjà effectuée sur les deux périphériques.

Utilisez le groupe broadcast-underlay configuré pour l'instance L2LISP et l'adresse IP L2Border Loopback0 pour vérifier l'entrée d'inondation de couche 2 (S, G) qui reliera ce paquet à d'autres noeuds de fabric. Consultez les tables mroute et mfib pour valider les paramètres tels que l'interface entrante, la liste des interfaces sortantes et les compteurs de transfert.

<#root>

BorderCP-1#

show ip int loopback 0 | i Internet

Internet address is

192.168.0.201/32

```
BorderCP-1#
show run | se 8232

interface L2LISP0.8232

instance-id 8232

  remote-rloc-probe on-route-change
  service ethernet
   eid-table vlan
1031



broadcast-underlay 239.0.17.1

BorderCP-1#
show ip mroute 239.0.17.1 192.168.0.201 | be \(

(
192.168.0.201, 239.0.17.1
), 1w5d/00:02:52, flags: FTA
  Incoming interface:
Null0
, RPF nbr 0.0.0.0
          <-- Local S,G IIF must be Null0

  Outgoing interface list:

 TenGigabitEthernet1/0/42
, Forward/Sparse, 1w3d/00:02:52, flags:
<-- Edge1 Downlink
    TenGigabitEthernet1/0/43
, Forward/Sparse, 1w3d/00:02:52, flags:
<-- Edge2 Downlink


BorderCP-1#
show ip mfib 239.0.17.1 192.168.0.201 count

Forwarding Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kilobits per second
Other counts:      Total/RPF failed/Other drops(OIF-null, rate-limit etc)
Default
```

 13 routes, 6 (*,G)s, 3 (*,G/m)s
Group:

239.0.17.1

  Source:

192.168.0.201

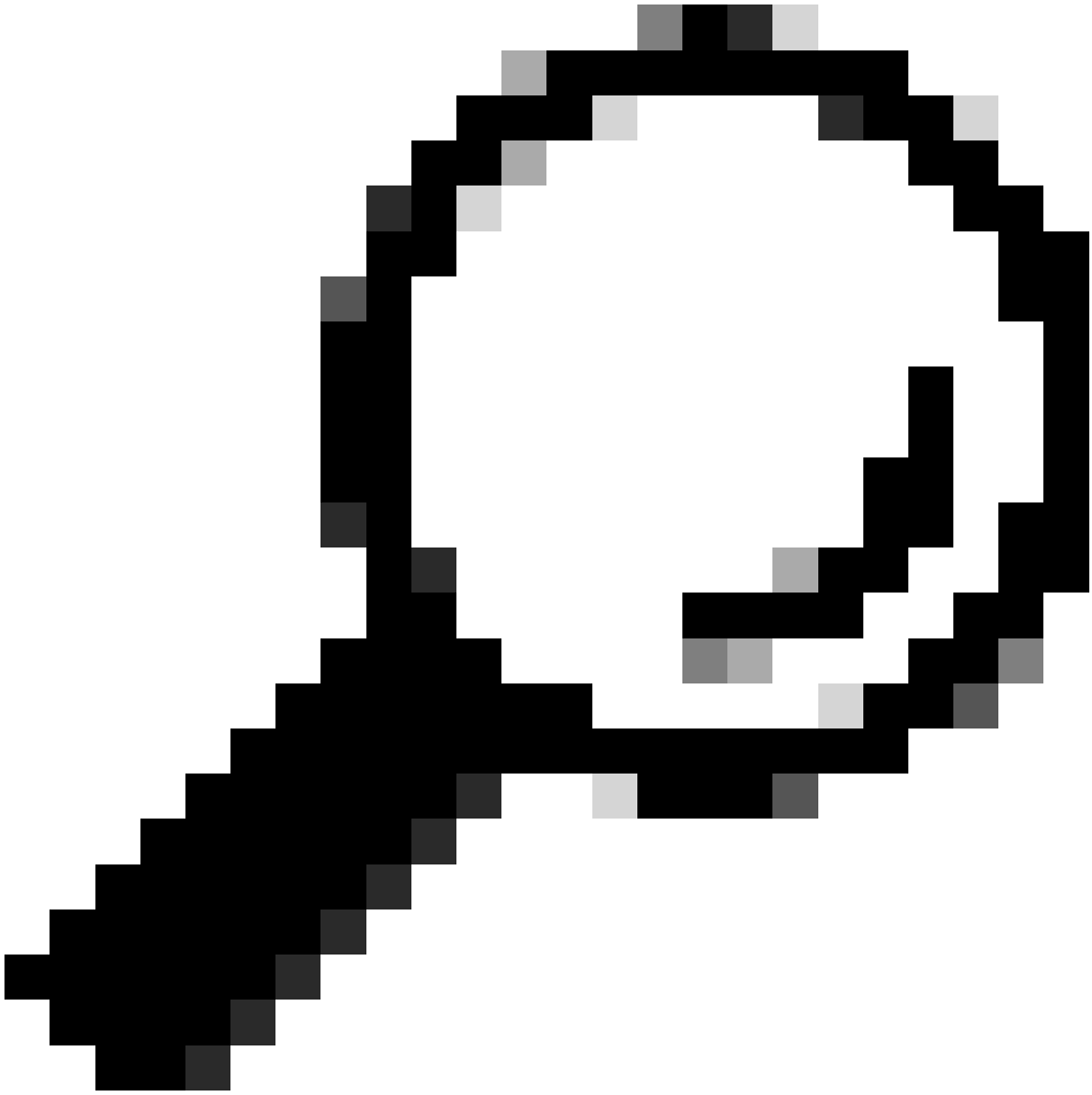
,
   SW Forwarding: 1/0/392/0, Other: 1/1/0
   HW Forwarding:

92071

/0/102/0, Other: 0/0/0

  <-- HW Forwarding counters (First counter = Pkt Count) must increase

  Totals - Source count: 1, Packet count: 92071



Conseil : Si aucune entrée (S, G) n'est trouvée ou si la liste d'interfaces sortantes (OIL) ne contient aucune interface sortante (OIF), cela indique un problème avec la configuration ou l'opération de multidiffusion sous-jacente.

Avec ces validations, ainsi que des captures de paquets similaires aux étapes précédentes, nous concluons cette section, car l'offre DHCP sera transférée en tant que diffusion à tous les Fabric Edge en utilisant le contenu de la liste d'interfaces sortantes, dans ce cas, hors de l'interface TenGig1/0/42 et TenGig1/0/43.

Offre DHCP et ACK - Diffusion - Périphérie

Exactement comme dans le flux précédent, nous vérifions maintenant le L2Border S, G dans le Fabric Edge, où l'interface entrante pointe vers le L2BN et l'OIL contient l'instance L2LISP mappée au VLAN 1031.

<#root>

Edge-1#show vlan id 1031

VLAN Name   Status   Ports
---- -------------------------------- --------- -------------------------------

1031

L2_Only_Wireless

active   L2LI0:

8232

, Te1/0/2, Te1/0/17, Te1/0/18, Te1/0/19, Te1/0/20,

Ac2

, Po1

Edge-1#

show ip mroute 239.0.17.1 192.168.0.201 | be \(

(

192.168.0.201

,

239.0.17.1

), 1w3d/00:01:52, flags: JT
  Incoming interface:

TenGigabitEthernet1/1/2

, RPF nbr 192.168.98.2

<-- IIF Te1/1/2 is the RPF interface for 192.168.0.201 (L2BN RLOC)a

  Outgoing interface list:

L2LISP0.8232

, Forward/Sparse-Dense, 1w3d/00:02:23, flags:

Edge-1#

show ip mfib 239.0.17.1 192.168.0.201 count

Forwarding Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kilobits per second
Other counts: Total/RPF failed/Other drops(OIF-null, rate-limit etc)
Default
 13 routes, 6 (*,G)s, 3 (*,G/m)s
Group:

 239.0.17.1

```
  Source:
```

192.168.0.201,

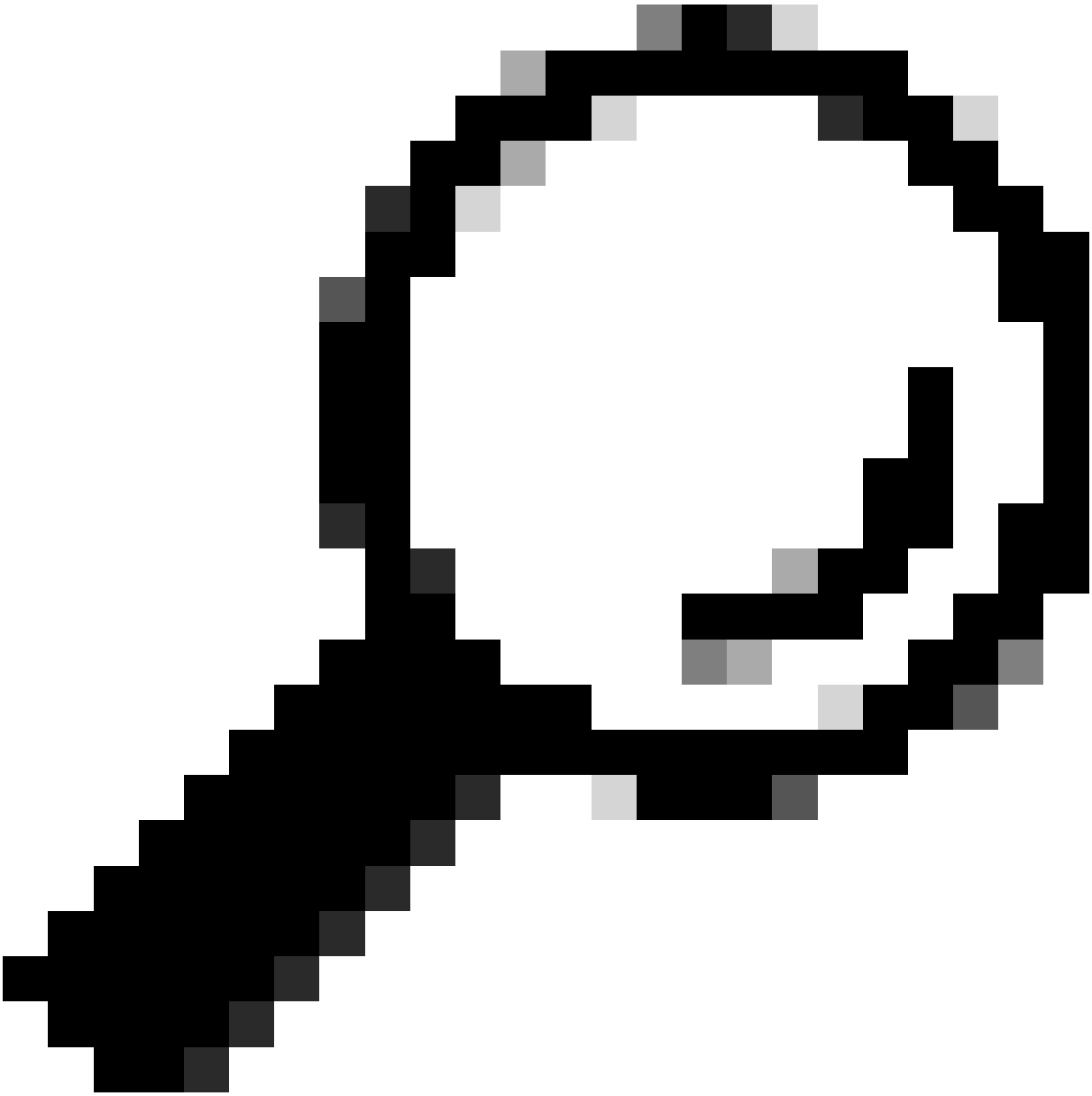
```
   SW Forwarding: 1/0/96/0, Other: 0/0/0
   HW Forwarding:
```

76236

```
/0/114/0, Other: 0/0/0
```

<-- HW Forwarding counters (First counter = Pkt Count) must increase

```
  Totals - Source count: 1, Packet count: 4
```



Conseil : Si une entrée (S, G) est introuvable, cela indique un problème avec la

---

configuration ou l'opération de multidiffusion sous-jacente. Si le L2LISP de l'instance requise n'est pas présent en tant qu'OIF, cela indique un problème avec l'état de fonctionnement UP/DOWN de la sous-interface L2LISP ou l'état d'activation IGMP de l'interface L2LISP.

La validation des listes de contrôle d’accès L2LISP est déjà effectuée sur les deux périphériques.

Une fois que le paquet est désencapsulé et placé sur le VLAN correspondant à VNI 8232, sa nature de diffusion indique qu'il est diffusé par tous les ports de transfert du protocole Spanning Tree filaire pour VLAN1031.

<#root>

```
Edge-1#
show spanning-tree vlan 1041 | be Interface

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------

Te1/0/2
         Desg
FWD
 20000     128.2    P2p Edge
Te1/0/17            Desg
FWD
 2000      128.17   P2p
Te1/0/18            Back
BLK
 2000      128.18   P2p
Te1/0/19            Desg
FWD
 2000      128.19   P2p
Te1/0/20            Back
BLK
 2000      128.20   P2p
```

Cependant, l'interface que nous recherchons pour diffuser l'offre DHCP est l'interface de tunnel d'accès associée au point d'accès. Cela est possible uniquement parce que « flood access-tunnel » est activé sur l'ID L2LISP 8232, sinon ce paquet est bloqué pour être transféré à l'interface AccessTunnel.

<#root>

```
Edge-1#
show lisp instance-id 8232 ethernet | se Multicast Flood

  Multicast Flood Access-Tunnel:
enabled

    Multicast Address:
232.255.255.1

    Vlan ID:
1021


Edge-1#
show ip igmp snooping  groups vlan 1021 232.255.255.1

Vlan      Group                   Type        Version     Port List
------------------------------------------------------------------------------

1021      232.255.255.1
         igmp        v2
Te1/0/12    <-- AP1 Port
```

Avec l'entrée de surveillance IGMP pour le groupe d'inondation de multidiffusion, les offres DHCP et les ACK sont transférés au port physique de l'AP.

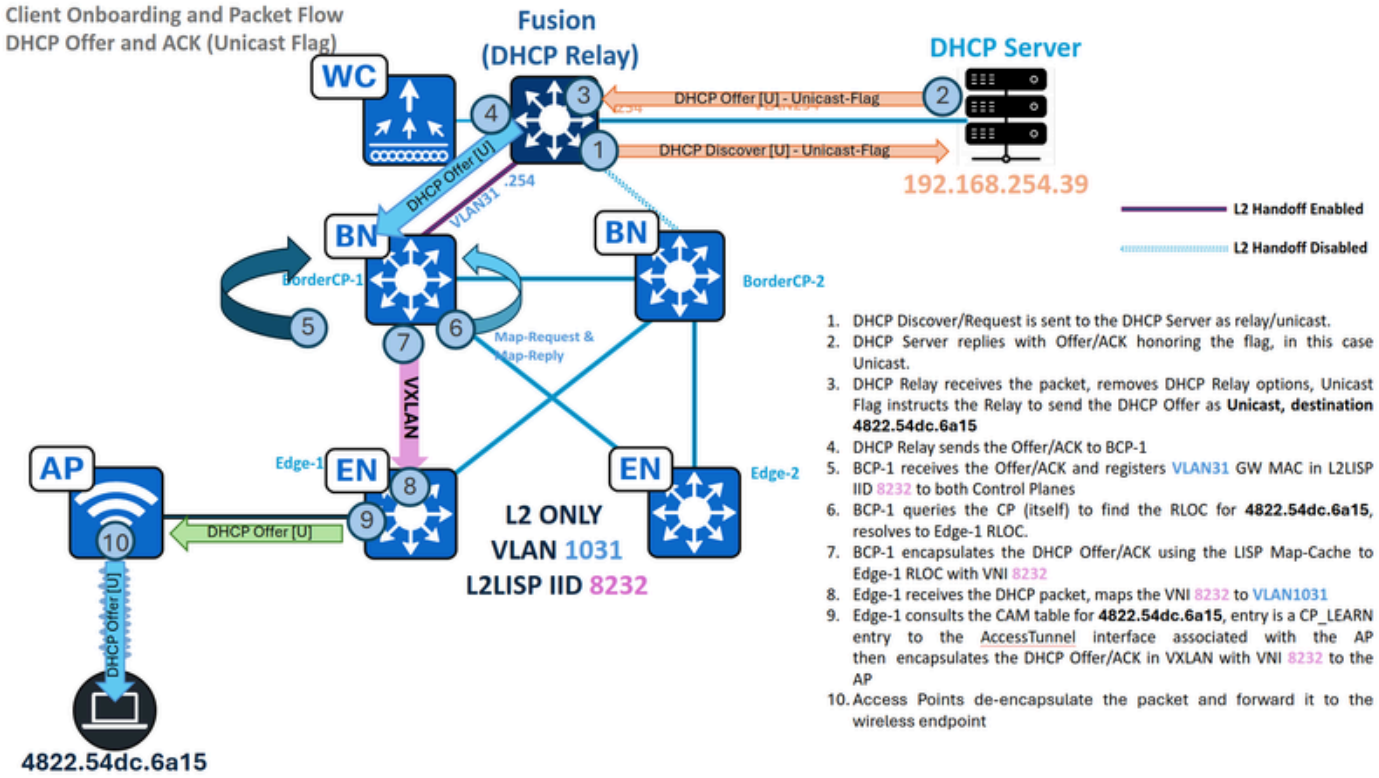
L'offre DHCP et le processus ACK restent cohérents. Si la surveillance DHCP n'est pas activée, aucune entrée n'est créée dans la table de surveillance DHCP. Par conséquent, l'entrée Device-Tracking pour le point d'extrémité DHCP est générée par des paquets ARP glanés. Il est également prévu que les commandes telles que « show platform dhcpsnooping client stats » n'affichent aucune donnée, car la surveillance DHCP est désactivée.

<#root>

```
Edge-1#
show device-tracking database interface Ac2 | be Network

   Network Layer Address                  Link Layer Address
Interface  vlan       prlvl      age        state      Time left

ARP


172.16.131.4
```

```
 4822.54dc.6a15


Ac2


1031
       0005       45s        REACHABLE  207 s try 0

Edge-1#show ip dhcp snooping  binding vlan 1041

MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----  --------------------

Total number of bindings: 0
```

Offre DHCP et ACK - Monodiffusion - Limite L2



Flux de trafic - Offre DHCP monodiffusion et ACK dans L2 uniquement

Ici, le scénario est un peu différent, le point d'extrémité définit l'indicateur de diffusion DHCP comme unset ou "0".

Le relais DHCP n'envoie pas l'offre DHCP/ACK en tant que diffusion, mais en tant que paquet de monodiffusion, avec une adresse MAC de destination dérivée de l'adresse matérielle du client à

l'intérieur de la charge utile DHCP. Cela modifie radicalement la façon dont le paquet est géré par le fabric SD-Access, il utilise le Map-Cache L2LISP pour transférer le trafic, et non la méthode d'encapsulation multicast de diffusion de couche 2.

Capture de paquets Fabric Border/CP (192.168.0.201) : Offre DHCP entrante

<#root>

```
BorderCP-1#

show monitor capture cap buffer display-filter "bootp.type==1 and
dhcp.hw.mac_addr==4822.54dc.6a15" detailed | sect Dynamic


Dynamic Host Configuration Protocol (

Discover

)
    Message type: Boot Request (1)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x00002030
    Seconds elapsed: 0

    Bootp flags: 0x0000, Broadcast flag (Unicast)


        0... .... .... .... = Broadcast flag: Unicast


        .000 0000 0000 0000 = Reserved flags: 0x0000
    Client IP address: 0.0.0.0
    Your (client) IP address: 0.0.0.0
    Next server IP address: 0.0.0.0
    Relay agent IP address: 0.0.0.0


Client MAC address: 48:22:54:dc:6a:15 (48:22:54:dc:6a:15)
```

Dans ce scénario, l'inondation de couche 2 est utilisée exclusivement pour la détection/les demandes, tandis que les offres/accusés de réception sont transférés via des caches de mappage L2LISP, ce qui simplifie le fonctionnement global. Conformément aux principes de transmission monodiffusion, la limite L2 interroge le plan de contrôle pour obtenir l’adresse MAC de destination. En supposant que "MAC Learning and WLC Notification" réussisse sur la périphérie du fabric, cet ID de point de terminaison (EID) est enregistré sur le plan de contrôle.

<#root>

```
BorderCP-1#

show lisp instance-id 8232 ethernet server 4822.54dc.6a15
```

```
LISP Site Registration Information
Site name: site_uci
Description: map-server configured from Catalyst Center
Allowed configured locators: any
Requested EID-prefix:
  EID-prefix:
```

4822.54dc.6a15/48

```
 instance-id 8232
    First registered:     00:53:30
    Last registered:      00:53:30
    Routing table tag:    0
    Origin:               Dynamic, more specific of any-mac
    Merge active:         No
    Proxy reply:          Yes
    Skip Publication:     No
    Force Withdraw:       No
```

TTL: **1d00h**

State: **complete**

```
    Extranet IID:         Unspecified
```

Registration errors:

Authentication failures: 0

Allowed locators mismatch: 0

```
    ETR 192.168.0.101:51328, last registered 00:53:30, proxy-reply, map-notify
                             TTL 1d00h, no merge, hash-function sha1
                             state complete, no security-capability
                             nonce 0xBB7A4AC0-0x46676094
                             xTR-ID 0xDEF44F0B-0xA801409E-0x29F87978-0xB865BF0D
                             site-ID unspecified
                             Domain-ID 1712573701
                             Multihoming-ID unspecified
                             sourced by reliable transport
      Locator        Local  State      Pri/Wgt  Scope
      192.168.0.101  yes    up           10/10   IPv4 none
```

ETR 192.168.254.69:58507

```
, last registered 00:53:30, no proxy-reply, no map-notify
```

<-- Registered by the Wireless LAN Controller

```
                              TTL 1d00h, no merge, hash-function sha2
```

state complete

```
, no security-capability
                              nonce 0x00000000-0x00000000
```

```
                              xTR-ID N/A
                              site-ID N/A
                              sourced by reliable transport
                              Affinity-id: 0 , 0
```

WLC AP bit: Clear

```
      Locator        Local  State      Pri/Wgt  Scope
```

192.168.0.101

```
 yes
```

up

```
         0/0    IPv4 none
```

<-- RLOC of Fabric Edge with the Access Point where the endpoint is connected

Après la requête du Border au Control Plane (local ou distant), la résolution LISP établit une entrée Map-Cache pour l'adresse MAC du point d'extrémité.

<#root>

```
BorderCP-1#
```

show lisp instance-id 8232 ethernet map-cache 4822.54dc.6a15

```
LISP MAC Mapping Cache for LISP 0 EID-table Vlan
```

31

```
 (IID
```

8232

```
), 1 entries
```

4822.54dc.6a15/48

```
, uptime: 4d07h, expires: 16:33:09,
```

via map-reply

```
,
```

complete

```
, local-to-site
  Sources: map-reply
  State: complete, last modified: 4d07h, map-source: 192.168.0.206
  Idle, Packets out: 46(0 bytes), counters are not accurate (~ 00:13:12 ago)
  Encapsulating dynamic-EID traffic
  Locator        Uptime    State  Pri/Wgt     Encap-IID
```

192.168.0.101

```
 4d07h     up      10/10        -
```

Une fois le RLOC résolu, l'offre DHCP est encapsulée en monodiffusion et envoyée directement à Edge-1 à l'adresse 192.168.0.101, avec VNI 8240.

```
<#root>
BorderCP-1#
show mac address-table address aaaa.dddd.bbbb

          Mac Address Table
-------------------------------------------
Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

31

 4822.54dc.6a15

CP_LEARN

L2LI0

BorderCP-1#
show platform software fed switch active matm macTable vlan 141 mac aaaa.dddd.bbbb

VLAN
   MAC                  Type  Seq# EC_Bi  Flags  machandle
siHandle        riHandle         diHandle   *a_time  *e_time  ports
                   Con
-------------------------------------------------------------------------------------------------------

31    4822.54dc.6a15

  0x1000001    0      0    64  0x718eb52c48e8  0x718eb52c8b68  0x718eb44c6c18      0x0            0

 RLOC 192.168.0.101

adj_id 1044  No

BorderCP-1#
show ip route 192.168.0.101
```

```
Routing entry for 192.168.0.101/32
  Known via "
```

isis

```
", distance 115, metric 20, type level-2
  Redistributing via isis, bgp 65001T
  Advertised by bgp 65001 level-2 route-map FABRIC_RLOC
  Last update from 192.168.98.3 on TenGigabitEthernet1/0/42, 1w3d ago
  Routing Descriptor Blocks:
  * 192.168.98.3, from 192.168.0.101, 1w3d ago,
```

via TenGigabitEthernet1/0/42

```
      Route metric is 20, traffic share count is 1
```

Avec la même méthodologie que dans les sections précédentes, capturez le trafic entrant du relais DHCP et vers l'interface de sortie RLOC pour observer l'encapsulation VXLAN en monodiffusion vers le RLOC Edge.

Offre DHCP et ACK - monodiffusion - périphérie

Le périphérique reçoit l'offre DHCP/ACK de monodiffusion de la périphérie, désencapsule le trafic et consulte sa table d'adresses MAC pour déterminer le port de sortie correct. Contrairement aux offres/accusés de réception de diffusion, le noeud Edge transfère alors le paquet uniquement vers le tunnel d'accès spécifique où le point d'extrémité est connecté, plutôt que de l'inonder vers tous les ports.

La table d'adresses MAC identifie le port AccessTunnel2 comme étant notre port virtuel associé à AP1.

<#root>

Edge-1#show mac address-table address 4822.54dc.6a15

```
          Mac Address Table
-------------------------------------------
Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
```

1031

4822.54dc.6a15

CP_LEARN

Ac2

```
Edge-1#show interfaces accessTunnel 2 description

Interface                      Status         Protocol Description

Ac2

up             up

      Radio MAC: dc8c.37ce.58a0,

IP: 172.16.1.7



Edge-1#show device-tracking database address 172.16.1.7 | be Network

   Network Layer Address                    Link Layer Address
Interface  vlan       prlvl      age        state      Time left
DH4

 172.16.1.7

                            dc8c.3756.99bc

Te1/0/12

   1021       0024       6s         REACHABLE  241 s try 0(86353 s)

Edge-1#show cdp neighbors tenGigabitEthernet 1/0/12 | be Device

Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID

AP1              Ten 1/0/12

      119              R T   AIR-AP480 Gig 0
```

L'offre DHCP et le processus ACK restent cohérents. Si la surveillance DHCP n'est pas activée, aucune entrée n'est créée dans la table de surveillance DHCP. Par conséquent, l'entrée Device-Tracking du point d'extrémité DHCP est générée par des paquets ARP glanés, et non par DHCP. Il est également prévu que les commandes telles que « show platform dhcpsnooping client stats » n'affichent aucune donnée, car la surveillance DHCP est désactivée.

<#root>

```
Edge-1#show device-tracking database interface te1/0/2 | be Network

   Network Layer Address                    Link Layer Address
Interface  vlan       prlvl      age        state      Time left
```

```
ARP


172.16.141.1


 aaaa.dddd.bbbb

       Te1/0/2

1041

       0005       45s        REACHABLE  207 s try 0

Edge-1#show ip dhcp snooping  binding vlan 1041


MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----  --------------------

Total number of bindings: 0
```

Il est essentiel de noter que le fabric SD-Access n'influence pas l'utilisation de l'indicateur de monodiffusion ou de diffusion, car il s'agit uniquement d'un comportement de point d'extrémité. Bien que cette fonctionnalité puisse être remplacée par le relais DHCP ou par le serveur DHCP lui-même, les deux mécanismes sont essentiels pour un fonctionnement DHCP transparent dans un environnement L2 uniquement : Inondation de couche 2 avec multidiffusion sous-jacente pour les offres/accusés de réception de diffusion et enregistrement correct des terminaux dans le plan de contrôle pour les offres/accusés de réception de monodiffusion.

Transaction DHCP - Vérification sans fil

À partir du WLC, la transaction DHCP est surveillée via RA-Traces.

<#root>

```
WLC#debug wireless mac 48:22:54:DC:6A:15 to-file bootflash:client6a15


    RA tracing start event,
       conditioned on MAC address: 48:22:54:dc:6a:15
       Trace condition will be automatically stopped in 1800 seconds.
       Execute 'no debug wireless mac 48:22:54:dc:6a:15' to manually stop RA tracing on this condition.


WLC#no debug wireless mac 48:22:54:dc:6a:15

    RA tracing stop event,
       conditioned on MAC address: 48:22:54:dc:6a:15


WLC#more flash:client6a15 | i DHCP


2025/08/11 06:13:48.600929726 {wncd_x_R0-0}{1}: [sisf-packet] [15981]: (info): RX: DHCPv4 from interfac
```

SISF_DHCPDISCOVER

, giaddr: 0.0.0.0, yiaddr: 0.0.0.0, CMAC: 4822.54dc.6a15
2025/08/11 06:13:50.606037404 {wncd_x_R0-0}{1}: [sisf-packet] [15981]: (info): RX: DHCPv4 from interfac

SISF_DHCPOFFER

, giaddr: 172.16.131.254, yiaddr: 172.16.131.4, CMAC: 4822.54dc.6a15
2025/08/11 06:13:50.609855406 {wncd_x_R0-0}{1}: [sisf-packet] [15981]: (info): RX: DHCPv4 from interfac

SISF_DHCPREQUEST

, giaddr: 0.0.0.0, yiaddr: 0.0.0.0, CMAC: 4822.54dc.6a15
2025/08/11 06:13:50.613054692 {wncd_x_R0-0}{1}: [sisf-packet] [15981]: (info): RX: DHCPv4 from interfac

SISF_DHCPACK

, giaddr: 172.16.131.254, yiaddr: 172.16.131.4, CMAC: 4822.54dc.6a15

À la fin de la transaction, le terminal est ajouté à la base de données Device-Tracking sur le contrôleur LAN sans fil.

<#root>

WLC#show wireless device-tracking database mac 4822.54dc.6a15

MAC	VLAN	IF-HDL	IP	ZONE-ID/VRF-NAME
4822.54dc.6a15				
1	0x90000006			
172.16.131.4		0x00000000		
			fe80::b070:b7e1:cc52:69ed	0x80000001

Toute la transaction DHCP est déboguée sur le point d'accès lui-même.

<#root>

AP1#debug client 48:22:54:DC:6A:15

AP1#term mon

AP1#
Aug 11 05:37:47 AP1 kernel: [*08/11/2025 05:37:47.3530] [1754890667:353058] [AP1] [48:22:54:dc:6a:15] <

[U:W]

DHCP_DISCOVER

: TransId 0x76281006
Aug 11 05:37:47 AP1 kernel: [*08/11/2025 05:37:47.3531] chatter: dhcp_req_local_sw_nonat: 1754890667.35
Aug 11 05:37:47 AP1 kernel: [*08/11/2025 05:37:47.3533] chatter: dhcp_from_inet: 1754890667.353287600: (
Aug 11 05:37:47 AP1 kernel: [*08/11/2025 05:37:47.3533] chatter: dhcp_reply_nonat: 1754890667.353287600
Aug 11 05:37:49 AP1 kernel: [*08/11/2025 05:37:49.3587] chatter: dhcp_from_inet: 1754890669.358709760: 1
Aug 11 05:37:49 AP1 kernel: [*08/11/2025 05:37:49.3588] chatter: dhcp_reply_nonat: 1754890669.358709760
Aug 11 05:37:49 AP1 kernel: [*08/11/2025 05:37:49.3589] [1754890669:358910] [AP1] [48:22:54:dc:6a:15]

[D:W]

DHCP_OFFER

: TransId 0x76281006 tag:534

Aug 11 05:37:49 AP1 kernel: [*08/11/2025 05:37:49.3671] [1754890669:367110] [AP1] [48:22:54:dc:6a:15] <

[U:W] DHCP_REQUEST

: TransId 0x76281006
Aug 11 05:37:49 AP1 kernel: [*08/11/2025 05:37:49.3671] chatter: dhcp_req_local_sw_nonat: 1754890669.367
Aug 11 05:37:49 AP1 kernel: [*08/11/2025 05:37:49.3709] [1754890669:370945] [AP1] [48:22:54:dc:6a:15]

[D:W]

DHCP_ACK

: TransId 0x76281006 tag:536

Aug 11 05:37:49 AP1 kernel: [*08/11/2025 05:37:49.3733] [1754890669:373312] [AP1] [48:22:54:dc:6a:15] <

[D:A] DHCP_OFFER

: TransId 0x76281006 [

Tx Success

] tag:534
Aug 11 05:37:49 AP1 kernel: [*08/11/2025 05:37:49.3983] [1754890669:398318] [AP1] [48:22:54:dc:6a:15] <

[D:A]

DHCP_ACK

: TransId 0x76281006 [

Tx Success

] tag:53

*** U:W = Uplink Packet from Client to Wireless Driver**

*** D:W = Downlink Packet from Client to Click Module**

*** D:A = Downlink Packet from Client sent over the air**

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.